

PCT

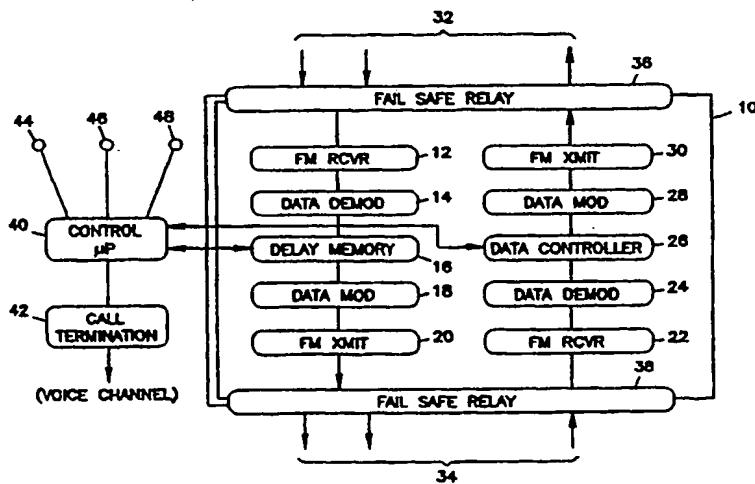
WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04Q 7/30		A1	(11) International Publication Number: WO 95/01707 (43) International Publication Date: 12 January 1995 (12.01.95)
(21) International Application Number: PCT/US94/02503		(81) Designated States: CA, JP, KR, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).	
(22) International Filing Date: 8 March 1994 (08.03.94)		Published <i>With international search report.</i>	
(30) Priority Data: 08/084,367 29 June 1993 (29.06.93)		US	
(71) Applicant: PACTEL CORPORATION [US/US]; 2999 Oak Road, M.S. 800, Walnut Creek, CA 94596 (US).			
(72) Inventors: RUDOKAS, Ronald, Steven; 177 Hemme, Alamo, CA 94507 (US). STORCH, John, Adam; 82 Fairlane Road, Laguna Niguel, CA 92677 (US). DANIELS, David, Leighton; 800 Magnolia, Placentia, CA 92670 (US).			
(74) Agent: BRUESS, Steven, C.; Merchant, Gould, Smith, Edell, Welter & Schmidt, 3100 Norwest Center, 90 South Seventh Street, Minneapolis, MN 55402 (US).			

(54) Title: FRAUD CONTROL IN CELLULAR TELEPHONE SYSTEMS



(57) Abstract

A method and apparatus for fraud control in cellular telephone systems. Call records from a switch are scanned to identify a fraudulent cellular phone based on its behavior. An identifier, e.g., a radio frequency (RF) signature, representative of the fraudulent phone is stored in a control channel editor (10) at a cell site. A database of identifiers may comprise a positive validation database storing the identifiers for all valid phones used in the cellular telephone system, or it may be a negative validation database storing the identifiers for known fraudulent phones. A control channel editor (10) intercepts a call origination request transmitted by a phone, and a control processor (40) compares one or more characteristics of the phone transmitting the call origination request to the database of identifiers. The control processor (40) then prevents the call origination request from completing when the comparison indicates that the phone is fraudulent. The call origination request can be prevented from completing by (1) re-routing the call to a customer service or "fraud hot line" number, (2) interrupting the call origination request, (3) transmitting a "hang-up" message to the phone, (4) transmitting a "hang-up" message to the cell site, or (5) transmitting a "tear-down" message to a switch.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	GB	United Kingdom	MR	Mauritania
AU	Australia	GE	Georgia	MW	Malawi
BB	Barbados	GN	Guinea	NE	Niger
BE	Belgium	GR	Greece	NL	Netherlands
BF	Burkina Faso	HU	Hungary	NO	Norway
BG	Bulgaria	IE	Ireland	NZ	New Zealand
BJ	Benin	IT	Italy	PL	Poland
BR	Brazil	JP	Japan	PT	Portugal
BY	Belarus	KE	Kenya	RO	Romania
CA	Canada	KG	Kyrgyzstan	RU	Russian Federation
CF	Central African Republic	KP	Democratic People's Republic of Korea	SD	Sudan
CG	Congo	KR	Republic of Korea	SE	Sweden
CH	Switzerland	KZ	Kazakhstan	SI	Slovenia
CI	Côte d'Ivoire	LI	Liechtenstein	SK	Slovakia
CM	Cameroon	LK	Sri Lanka	SN	Senegal
CN	China	LU	Luxembourg	TD	Chad
CS	Czechoslovakia	LV	Latvia	TG	Togo
CZ	Czech Republic	MC	Monaco	TJ	Tajikistan
DE	Germany	MD	Republic of Moldova	TT	Trinidad and Tobago
DK	Denmark	MG	Madagascar	UA	Ukraine
ES	Spain	ML	Mali	US	United States of America
FI	Finland	MN	Mongolia	UZ	Uzbekistan
FR	France			VN	Viet Nam
GA	Gabon				

FRAUD CONTROL IN CELLULAR TELEPHONE SYSTEMS

BACKGROUND OF THE INVENTION

1. Field of the Invention.

5 This invention relates in general to radio frequency (RF) communication systems, and in particular, to a method and apparatus for fraud control in cellular mobile radiotelephone (CMR) and personal communications services (PCS) systems.

10

2. Description of Related Art.

Cellular telephones combine the mobility of the radio link and the world-wide land telephone network to provide a communication link to any other telephone in 15 the world. However, as cellular phones have become more prevalent throughout the country, fraud has become a major problem. Cellular fraud robs service providers of hundreds of millions of dollars every year. Like all crimes, there are several varieties of cellular fraud, 20 including "cloning."

Cloning fraud, which occurs when a legitimate subscriber's MIN/ESN combination is used for illegal purposes, is among the most sophisticated and difficult forms of fraud to prevent. Often, the pirate will use 25 simple electronic devices to "capture" the legitimate MIN/ESN combination during its transmission by radio frequency (RF). In these cases, the legitimate subscriber often does not know fraud is being committed with his or her MIN/ESN combination until they receive 30 the bill. This is currently the most popular method of gaining illegal access to a cellular system, because the legitimacy of the stolen MIN/ESN combinations makes cloning difficult to catch.

There are certain steps that can be taken to prevent 35 cloning fraud. In some instances, carriers block calls to certain destinations, or impose "brownouts" on calls using specified MIN codes, particularly on international calls, that have been previously abused. Although

drastic, this method currently is often the only way to stop cloning fraud.

The eventual release of digital cellular phones into the mass market will provide another avenue for fraud.

5. Digital phones will also be susceptible to new and improved criminal techniques for stealing MIN/ESN combinations. Thus, carriers are forced to seek other methods of detecting and preventing fraudulent calls.

Several companies, including Electronic Data Systems (EDS) and Subscriber Computing, Inc. (SCI) have developed anti-cloning products that analyze calling patterns using call records. For example, EDS' PCC Cloning Detection System and SCI's Fraud Watch System are designed to be interfaced with cellular switches, so that call information can be collected after the calls have been completed. These systems can be used to identify calling patterns in the collected information that indicate fraudulent usage.

These systems typically allow operators to specify certain criteria to identify fraud. These criteria may include number of calls per hour, call durations, number of minutes used by a specific phone within an hour, number of international or toll calls per hour, and calls to specific countries or NPA/NXXX codes. Operator 25 can also identify fraudulent usage by the specific number dialed for those numbers that have been previously identified as a number called by fraudulent callers. The call records of cellular phones meeting any number of criteria can be viewed online or printed.

30. Although they cannot prevent cloning fraud, such systems provide carriers with a method of identifying cloning fraud, so that losses can be tabulated. Unfortunately, current methods can only detect or monitor fraud after the caller hangs up, and provide no 35 way to stop fraud. Thus, there is a need in the art for techniques that enhance the use of analyzed call

patterns to deny pirates the use of cellular telephone systems.

SUMMARY OF THE INVENTION

5 To overcome the limitations in the prior art described above, and to overcome other limitations that will become apparent upon reading and understanding the present specification, the present invention discloses a method and apparatus for fraud control in RF
10 communications systems, and cellular telephone systems in particular. Call records are scanned to identify a fraudulent cellular phone based on its behavior. An identifier, for example, an RF signature, representative of the fraudulent cellular phone is stored in fraud
15 control equipment located at a cell site. A database of identifiers may comprise a positive validation database storing the identifiers for all valid cellular phones used in the cellular telephone system, or it may be a negative validation database storing the identifiers for known fraudulent cellular phones. A control channel
20 editor intercepts a call origination request transmitted from a cellular phone to the cell site, and compares one or more characteristics of the cellular phone transmitting the call origination request to the
25 database of identifiers. The control channel editor then prevents the completion of the phone call when the comparison indicates that the cellular phone is fraudulent. The call origination request can be prevented from completing by (1) re-routing the call to
30 a customer service or "fraud hot line" number, (2) interrupting the call origination request, (3) transmitting a "hang-up" message to the phone, (4) transmitting a "hang-up" message to the cell site, or (5) transmitting a "tear-down" message to a switch.

BRIEF DESCRIPTION OF THE DRAWINGS

Referring now to the drawings in which like reference numbers represent corresponding elements throughout:

5 Figure 1 is a block diagram illustrating the components of the present invention;

Figure 2 is a block diagram illustrating the components of the present invention including an emitter detect; and

10 Figure 3 is a block diagram further illustrating the components of the centralized fraud control system used in the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

15 In the following description of the preferred embodiment, reference is made to the accompanying drawings which form a part hereof, and in which is shown by way of illustration, a specific embodiment in which the invention may be practiced. It is to be understood that other embodiments may be used and changes may be made without departing from the scope of the present invention.

Overview

25 The present invention provides a method and apparatus for fraudulent control in controlled access wireless communications systems, including cellular mobile radiotelephone (CMR) systems, personal communications services (PCS) systems, and specific 30 multiuser radio (SMR) systems. The present invention identifies fraudulent cellular phones by past behavior and a unique identifier, and then denies these cellular phones any further use of the cellular network. The present invention also has application to system 35 monitoring of cell site and subscriber phone performance, cellular phone location services, and other applications.

Figure 1 is a block diagram illustrating a component of the present invention. A control channel editor 10 comprises receive side components including an FM receiver 12, data demodulator 14, delay memory logic 16, data modulator 18 and an FM transmitter 20, and transmit side components including an FM receiver 22, data demodulator 24, data controller 26, data modulator 28 and an FM transmitter 30.

The control channel editor 10 is coupled to the RF distribution cabling from the cell site antennae 32 and to the cell site control channel equipment 34. Since the control channel editor 10 deals with a standard RF interface, it can be used with any cell site equipment 34. Moreover, the operation of the control channel editor 10 is transparent to cellular phone users during normal operation, and acts only to interrupt the placement of calls by fraudulent cellular phones.

In order to provide the level of reliability required in a public service system, fail-safe relays 36 and 38 are provided to allow normal operation of the cell site equipment should a malfunction occur within the control channel editor 10. If the control channel editor 10 fails in any way, the relays 36 and 38 will be de-energized, so that control channel editor 10 is bypassed.

A control processor 40 is coupled to the control channel editor 10 via the delay memory logic 12 and the data controller 26. Also coupled to the control processor is a call termination signal generator 42, an RF signature system 44, a switch 46, and a centralized fraud control system 48.

Upon further reading of this specification, those skilled in the art will recognize that not all of the various components shown in Figure 1 are required to practice the present invention. Moreover, different combinations of the components from those illustrated herein may be used, as described in more detail below.

In addition, the connections between components made be modified from those illustrated herein, depending on the method of fraud control used.

5

Operation

When a user first turns on his cellular telephone, the cellular phone scans and identifies the set-up or control channels being received. The cellular phone then selects and tunes to the strongest control channel signal, presumably from the nearest cell transmitter. Transmitted "busy-idle" bits inform the cellular phone of the status of the reverse signalling portion (phone to cell site) of the control channel to prevent simultaneous seizure by more than one cellular phone.

15 There are other handshake and timing checks to guard against collisions between cellular phones.

The cellular phone automatically registers with the cellular system when it is powered on. At registration, the phone sends its mobile identification number (MIN), electronic serial number (ESN), station class mark, etc., to the cell site. Depending upon system procedures, registration can verify that service for the cellular phone is available, or that the cellular phone is not on a "hot list" relating to unauthorized use or 25 stolen phones. However, unless the MIN/ESN combination is on the "hot list," registration will not identify cloning fraud. After registration, the cellular phone then turns-off its transmitter, although it continues to monitor the selected control channel for incoming calls.

30 When a call is originated from the cellular phone, the subscriber enters the dialed digits of the called number, which are temporarily stored in the cellular phone, and presses the "send" key. The cellular phone then goes "off-hook," and scans and selects the 35 strongest control channel. When a "busy-idle" bit signifies that the control channel is idle, the phone sends a data stream to the cell site, including its

identification (MIN/ESN) and the dialed digits of the called number.

In one embodiment of the present invention, the signalling data stream from the cellular phone is received as RF signals at the antennae 32 of the cell site. The RF signals are coupled from the antennae 32 to the FM receiver 12, and then demodulated by data demodulator 14. At the appropriate time, the transmit side components of the control channel editor 10 toggle the busy/idle bit in the signalling data stream to the cellular phone. This "handshake" lets the cellular phone know that the cell site is receiving the control signal. The data stream is then stored at delay memory logic 16, so that the call origination request represented thereby can be delayed if necessary until the identity of the cellular phone is verified. The data stream is also transmitted to the control microprocessor 40, which uses one or more of a plurality of identification techniques to determine whether the cellular phone is fraudulent. After the control microprocessor 40 completes its identification, and has determined that the cellular phone is not fraudulent, the data stream is re-modulated by data modulator 18 to the same frequency and then transmitted to a control channel transceiver component (not shown) of the cell site equipment 34 by the FM transmitter 20. To complete the call set-up, the control channel transceiver component of the cell site equipment 34 transmits the voice channel assignment to the transmit side components of the control channel editor 10. The transmit side components of the control channel editor 10 transmit the voice channel assignment to the cellular phone and to the control processor 40.

If the cellular phone is identified as fraudulent, then the control processor 40 and control channel editor 10 can use one or more of a plurality of different methods to handle the call origination. For example,

one method may completely interrupt or deny the call set-up, so that the data stream received from the cellular phone is not transmitted to the control channel transceiver of the cell site equipment 34. Another 5 method may alter the dialed phone number embedded in the data stream, so that the call is re-routed to a customer service phone number or "fraud hot line" phone number instead of the phone number dialed by the user. Both of 10 these methods would preferably use a fast identification technique in the control microprocessor 40, e.g., identification within 0.5 seconds, so that calls are not adversely affected by slow call origination response. Moreover, this method would require only the receive 15 side components of the control channel editor 10.

Still another method may send release, reorder, maintenance, or interrupt order commands to the cellular phone using the transmit side components of the control channel editor 10. While this method could be used with 20 a fast identification technique, it is also readily used with slower identification techniques, e.g., identification within one second. Moreover, this method would require both the receive side and transmit side 25 components of the control channel editor 10, although the receive side components may only need to "tap" into the reverse signalling data streams and may not have to delay and/or re-build the data streams.

Yet another method may transmit a call termination signal to a voice channel transceiver (not shown) of the cell site equipment 34 using the call termination signal 30 generator 42. The particular voice channel transceiver is identified by the voice channel assignment information provided to the control processor 40 by the transmit side components of the control channel editor 10. The call termination signal generator 42 instructs 35 the cell site equipment 34 that the user has "hung up" his phone, so that the cell site equipment 34 then also hangs up. While this method could be used with a fast

identification technique, it also permits the use of slower, more complex identification techniques, e.g., identification taking more than one second. Moreover, the call termination could occur at any point during the 5 call, so there is no time limit for the identification techniques. However, the method generates call records that will need to be resolved during the billing cycle to avoid billing the valid customers for the fraudulent calls.

10 Still yet another method may transmit a call termination command to the switch 46 from the control microprocessor 40. This command would instruct the switch 46 to terminate the call. While this method could be used with a fast identification technique, it 15 also permits the use of slower, more complex identification techniques, e.g., identification taking more than one second. The call termination could occur at any point during the call, so there is no time limit for the identification techniques. Moreover, this 20 method may only require the receive side components of the control channel editor 10 for "tapping" the signalling data stream from the cellular phone, and thus may not have to delay and/or re-build the data streams. However, the method generates call records that will 25 need to be resolved during the billing cycle to avoid billing the valid customers for the fraudulent calls.

The identification techniques performed by the control microprocessor 40 would compare the cellular phone placing the call against an identification 30 database. These comparisons may be performed against a negative validation database (containing known fraudulent cellular phones) or a positive validation database (containing all known non-fraudulent cellular phones). Typically, a negative validation database 35 would be preferred, because it would be smaller and more readily searched, thereby limiting the amount of time the comparison would require. Moreover, with the

negative validation database, secondary pattern data, such as call history, called number, call frequency, call time, station, class, etc., can be used to validate a close match.

5 The identification techniques performed by the present invention can comprise one or more of a plurality of different methods. For example, known "cloned" MIN/ESN combinations can be denied access to the cellular telephone system, although this is easily
10 circumvented by the pirate re-programming the fraudulent cellular phone. Another technique would use the MIN/ESN combination to look-up one or more known station class marks of the corresponding cellular phone, compare the known station class marks to the station class mark
15 transmitted to the cell site by the cellular phone, and deny access when a mismatch occurs. Still another technique would compare the dialed phone digits to "suspect" phone numbers uncovered during the analysis of prior fraudulent cellular phone calls, and deny calls
20 placed to those suspect phone numbers.

An identification technique based on the comparison of RF signatures for the cellular phones could also be used to identify fraudulent cellular phones. The use of RF signature identification is important because it
25 provides a way of independently identifying the fraudulent phone with using the ESN or MIN. Moreover, the use of RF signature identification can be used nationally to prevent roaming fraud.

30

RF Signature Identification

Figure 2 is a block diagram further illustrating the components of the RF signature system 44. The RF signature system 44 typically comprises an FM receiver 50, analog-to-digital (A/D) convertor 52, and a digital signal processor (DSP) 54. From existing antennae 32, the received RF signal is sent to the FM receiver 50 that operates in the 824 MHz to 894 MHz range and has

repeatable performance characteristics, including flat frequency and phase response, low phase noise, high dynamic range, stable amplitude, and accurate automatic gain control. The A/D convertor 52, which converts the analog output from the FM receiver 50 into digital data, preferably has a minimum sample rate of 3.2 MHz to accommodate a bandwidth greater than or equal to 1.25 MHz. The DSP 54 performs the necessary calculations using the digital output of the A/D convertor 52 to determine the RF signature of the cellular phone. The DSP 54 encodes measured characteristics of the cellular phone into a digital RF signature descriptor data stream.

The control microprocessor 40 compares the digital RF signature descriptor data stream to a database of RF signatures of known fraudulent cellular phones (negative validation) or with a database of RF signatures of all non-fraudulent cellular phones (positive validation). In a positive validation database, the combination of RF signature with the associated MIN/ESN combination would most likely prove to be "uncloneable." In a negative validation database, secondary pattern data, such as the cell site, MIN/ESN combination, call history, the called number, call frequency, call time, station, class, etc., can be used to validate a close match.

The technique of identifying an RF signature is not new in the art, and has been previously used in military and intelligence applications. An example of an apparatus for characterizing a radio transmitter can be found in U.S. Patent No. 5,005,210 issued April 2, 1991, to Ferrell, incorporated by reference herein. Other examples include technology developed by the Electromagnetic Systems Laboratory of TRW, Inc.

The characteristics used in creating the RF signature should be consistent over time, temperature, battery voltage, orientation, location, use of car kits, etc., and yet be distinctive between individual cellular

phones. Usually, the RF signature can be any unintentional modulation that is unique to the specific cellular phone. Because of fading due to multipath transmissions, amplitude data will typically be 5 distorted, and thus the characteristics used should preferably comprise phase or frequency type characteristics that are less affected by the cellular environment.

These characteristics can include, but are not 10 limited to, turn-on transmitting amplitude, frequency or phase modulation versus time, the time between turn-on and onset of data, phase and frequency modulation during that delay, the initial amplitude, phase and frequency modulation when data transmission starts, transmission 15 bit times, total times, timing jitter, rise and fall timing, carrier turn-off time, modulation deviation and distortion, modulation phase, bit to bit modulation variations, demodulation spectrum, spurious transmitter data, etc.

20 Some or all of these various characteristics can be used by the DSP 54 to create an RF signature unique for a given cellular phone. Preferably, the DSP 54 then condenses the selected characteristics into a digital RF signature descriptor data stream having a compact format 25 that is easy to transmit from place to place. For example, the digital RF signature descriptor data stream can be transmitted to a control processor 40 and centralized fraud control system 48 for storage and later inclusion into positive and negative validation 30 databases.

Centralized Fraud Control System

Figure 3 is a block diagram further illustrating the components of the centralized fraud control system 48. 35 The fraud control system comprises a CPU 56, one or more monitors 58, a data link 60 to a port of the switch 46, a data link 62 to the control microprocessor 40, and

(optionally) databases for call records 64, RF signatures 66, positive validation 68 and negative validation 70.

The fraud control system 48 performs real-time data collection of call records from the cellular telephone switch 46 into a call database 64. Using a behavior profiling algorithm, the fraud control system 48 scans the call records in the database 64 and extracts records corresponding to probable fraudulent activity. The behavior profiling algorithm identifies and flags specific activities represented within the different fields of the call records, including time, duration, cell, dialed digits, etc. Relative probabilities are assigned to the specific activities identified and flagged within the call records.

Some example criteria and their relative probabilities are described below:

1. Excessive call duration threshold made by a cellular phone within a given time period. For example, more than one long duration call per hour could result in the assignment of 15 points towards an alarm threshold.
2. Excessive number of call attempts made by a cellular phone within a given time period. For example, more than one call attempt per hour could result in the assignment of 15 points towards an alarm threshold.
3. All domestic toll call attempts made by a cellular phone within a given time period. For example, each domestic toll call attempt per hour could result in the assignment of 13 points towards an alarm threshold.
4. All international toll call attempts made by a cellular phone within a given time period. For example, each international toll call attempt per hour could result in the assignment of 20 points towards an alarm threshold.

5. All three-way conference calls made by a cellular phone within a given time period. For example, each three-way conference call attempt per hour could result in the assignment of 17 points towards an alarm threshold.
10. Excessive number of call attempts to specific NPA/NXXX codes made by a cellular phone within a given time period. For example, more than one call attempt per hour could result in the assignment of 15 points towards an alarm threshold.
15. Any calls with identical MIN/ESN that overlap for more than 59 seconds. 100 points.
20. Any calls to a known phone number previously called by fraudulent cellular phones under the assumption that "who you call is who you are." 100 points.
25. Any calls from a cellular phone to the number of a known fraudulent cellular phone under the assumption (verified by a 70% correlation) that the cellular phone placing the call is fraudulent as well. 100 points.

These criteria and associated probabilities are the result of trial and error investigation by the Assignee, and have been validated through experience. Nonetheless, those skilled in the art will recognize that other criteria and probabilities could be substituted for those described above, without departing from the scope of the present invention.

30. The fraud control system 48 indexes all call records in the call database 64 linked to a specific MIN/ESN combination and the relative probabilities are accumulated towards an alarm threshold. The alarm threshold reflects an accumulated probability within some defined period, e.g., accumulating 100 probability points within one hour. The alarm threshold may be

reached immediately, as when one call overlaps another with an identical MIN for more than 59 seconds.

If the alarm threshold is reached, the MIN/ESN combination is identified as a fraudulent cellular

5 phone. In some cases, these identifications of fraudulent cellular phones are performed automatically by the fraud control system 48. In other cases, these identifications of fraudulent cellular phones are performed automatically by the fraud control system 48, 10 and then verified through the intervention of an operator.

Once a fraudulent cellular phone is identified by the fraud control system 48, the positive and/or negative validation databases 68 and 70 are updated to 15 reflect the identification. The updates may include all manner of phone-specific information, such as the RF signature from the RF signature database 66, and the MIN/ESN combination, the associated station class marks of the phone, "suspect" dialed numbers, etc., from the 20 call database 64 and/or a subscriber information database (not shown). In addition, the local database used by the control microprocessor 40 is updated to prevent further access by the fraudulent cellular phone.

25

Conclusion

This concludes the description of the preferred embodiment of the invention. The following paragraphs describe some alternative methods of accomplishing the same invention.

30 In addition to cellular telephone systems, those skilled in the art will recognize that the present invention can be applied to other mobile radios, personal communications systems, paging systems, aircraft communications, satellite communications, as 35 well any other controlled-access radio frequency communications systems.

Rather than using the specific components and combinations of components described herein, those skilled in the art will recognize that other components and combinations of components could be substituted therefor without departing from the scope of the present invention. Moreover, the connections between various components may be modified from those illustrated herein.

Rather than using the specific methods and process steps described herein, those skilled in the art will recognize that other methods and steps could be substituted therefor without departing from the scope of the present invention.

In summary, a method and apparatus for fraud control in cellular telephone systems has been described. Call records from a switch are scanned to identify a fraudulent cellular phone based on its behavior. An identifier, e.g., a radio frequency (RF) signature, representative of the fraudulent cellular phone is stored in a control channel editor at a cell site. A database of identifiers may comprise a positive validation database storing the identifiers for all valid subscribers of the cellular telephone system, or it may comprise a negative validation database storing the identifiers for known fraudulent cellular phones. A control channel editor intercepts a call origination request transmitted from a cellular phone to the cell site, and a control processor compares one or more characteristics of the cellular phone transmitting the call origination request to the database of identifiers. The control processor then prevents the call origination request from completing when the comparison indicates that the cellular phone is fraudulent. The call origination request can be prevented from completing by (1) re-routing the call to a customer service or "fraud hot line" number, (2) interrupting the call origination request, (3) transmitting a "hang-up" message to the

phone, (4) transmitting a "hang-up" message to the cell site, or (5) transmitting a "tear-down" message to a switch.

The foregoing description of the preferred embodiment of the invention has been presented for the purposes of illustration and description. It is not intended to be exhaustive or to limit the invention to the precise form disclosed. Many modifications and variations are possible in light of the above teaching. It is intended that the scope of the invention be limited not by this detailed description, but rather by the claims appended hereto.

WHAT IS CLAIMED IS:

1. An apparatus for preventing fraud in a radiotelephone system, comprising:

(a) a control channel editor, coupled to an antenna at a receiving site in the radiotelephone system, for receiving radio frequency (RF) signals from a radiotelephone comprising a call origination request; and

(b) a control processor, coupled to the control channel editor, for comparing a characteristic of the radiotelephone to stored identifiers when the call origination request is received by the control channel editor, for determining whether the radiotelephone is fraudulent based on the comparison, and for interrupting the call from the radiotelephone when the comparison indicates that the radiotelephone is fraudulent.

2. The invention as set forth in claim 1 above, wherein the means for interrupting comprises means for replacing a called number embedded in the call origination request received by the control channel editor with a predetermined fraud redirection number.

3. The invention as set forth in claim 1 above, wherein the means for interrupting comprises means for instructing the control channel editor to transmit a "hang-up" signalling tone to the cell site when the comparison indicates that the radiotelephone is fraudulent, so that the call is terminated.

4. The invention as set forth in claim 1 above, wherein the means for interrupting comprises means for instructing the control channel editor to transmit a command to the phone when the comparison indicates that the radiotelephone is fraudulent, so that the call is terminated, wherein the command is selected from a group

comprising release, reorder, maintenance and intercept order commands.

5. The invention as set forth in claim 1 above, wherein the control processor is coupled to a switch, and the means for interrupting comprises means for transmitting a "tear-down" message to the switch when the comparison indicates that the radiotelephone is fraudulent, so that the call is terminated.

6. The invention as set forth in claim 1 above, wherein the control channel editor comprises:

- (1) an FM receiver, coupled to an antenna at the receiving site, for receiving radio frequency (RF) signals from the radiotelephone transmitting the call origination request and for generating analog signals corresponding thereto;
- (2) a data demodulator, coupled to the FM receiver, for converting the analog signals into digital data;
- (3) delay memory logic, coupled to the data demodulator and the control processor, for delaying transmission of the digital data;
- (4) a data modulator, coupled to the delay memory, for converting the digital data into analog signals; and
- (5) an FM transmitter, coupled to a control channel transceiver at the receiving site, for receiving the analog signals and for transmitting radio frequency (RF) signals corresponding thereto to the control channel transceiver.

7. The invention as set forth in claim 6 above, wherein the control channel editor further comprises:

- (7) an FM receiver, coupled to the control channel transceiver at the receiving site, for receiving radio frequency (RF) signals from the control channel transceiver and for generating analog signals corresponding thereto, wherein the RF signals comprise

supervisory and control transmissions to the radiotelephone;

(7) a data demodulator, coupled to the FM receiver, for converting the analog signals into digital data;

(8) a data controller, coupled to the data demodulator and the control processor, for transmitting the digital data to the control processor;

(9) a data modulator, coupled to the data controller, for converting the digital data into analog signals; and

(10) an FM transmitter, coupled to the antenna at the receiving site, for receiving the analog signals and for transmitting radio frequency (RF) signals corresponding thereto to the radiotelephone.

8. The invention as set forth in claim 1 above, further comprising:

(c) an RF signature system, coupled to the control processor, for receiving a radio frequency (RF) transmission from the radiotelephone, and for characterizing the RF transmission as a digital RF signature substantially unique to the radiotelephone; and

(d) the control processor further comprising means for comparing the digital RF transmission to a database of stored digital RF signatures to determine whether the radiotelephone is fraudulent.

9. The invention as set forth in claim 8 above, wherein the database is a positive validation database comprising the digital RF signatures for all valid radiotelephones used in the cellular telephone system.

10. The invention as set forth in claim 8 above, wherein the database is a negative validation database comprising the digital RF signatures for known fraudulent radiotelephones.

11. The invention as set forth in claim 8 above, wherein the control processor further comprises means for comparing secondary patterns characteristic of the radiotelephone to stored identifiers of the secondary patterns to determine whether the radiotelephone is fraudulent when the comparison of the digital RF signature indicates a close, but not exact, match, wherein the secondary patterns comprise one or more of the following:

- a mobile identification number (MIN) transmitted from the radiotelephone,
- an electronic serial number (ESN) transmitted by the radiotelephone,
- a called number transmitted by the radiotelephone,
- a receiving site receiving the call origination request,
- a frequency of call origination requests received from the radiotelephone for a specified time period, and
- an amount of time the radiotelephone has been in use for a specified time period.

12. The invention as set forth in claim 1 above, further comprising:

(c) a fraud processor, coupled to the control processor and a switch, for receiving call records from the switch, for analyzing the call records to identify fraudulent phones based on the behavior described in the call records, and for transmitting an identifier representative of the fraudulent phone to the control processor.

13. A method for preventing fraudulent calls in a controlled access radiotelephone system, comprising the steps of:

(a) scanning call records from a switch to identify fraudulent radiotelephones based on their behavior;

(b) storing an identifier for each of the fraudulent radiotelephones in an electronic memory, wherein the identifier is representative of a characteristic of the fraudulent radiotelephone;

(c) receiving a call origination request transmitted from a radiotelephone to a cell site;

(d) detecting the characteristic of the radiotelephone transmitting the call origination request;

(e) comparing the characteristic of the radiotelephone transmitting the call origination request to the stored identifiers in the electronic memory; and

(f) preventing the call origination request from completing when the comparison indicates that the radiotelephone transmitting the call origination request is fraudulent.

14. The invention as set forth in claim 13 above, wherein the preventing step comprises the step of re-routing the call origination request when the comparison indicates that the radiotelephone is fraudulent, wherein a called number embedded in the call origination request is replaced with a predetermined fraud redirection number.

15. The invention as set forth in claim 13 above, wherein the preventing step comprises the step of interrupting the call origination request when the comparison indicates that the radiotelephone is fraudulent, so that the call origination is never completed.

16. The invention as set forth in claim 13 above, wherein the preventing step comprises the step of transmitting a "hang-up" signalling tone to the cell site when the comparison indicates that the

radiotelephone is fraudulent, so that the call is terminated.

17. The invention as set forth in claim 13 above, wherein the preventing step comprises the step of transmitting a command to the phone, when the comparison indicates that the radiotelephone is fraudulent, so that the call is terminated, wherein the command comprises at least one of the commands from a group comprising release, reorder, maintenance and intercept order commands.

18. The invention as set forth in claim 13 above, wherein the preventing step comprises the step of transmitting a "tear-down" message to a switch when the comparison indicates that the radiotelephone is fraudulent, so that the call is terminated.

19. The invention as set forth in claim 13 above, wherein the characteristic is a radio frequency (RF) signature, and the indicator is a digital value of the RF signature.

20. The invention as set forth in claim 13 above, wherein the identifier is a mobile identification number (MIN).

21. The invention as set forth in claim 13 above, wherein the identifier is an electronic serial number (ESN).

22. The invention as set forth in claim 13 above, wherein the identifier is a called number.

23. The invention as set forth in claim 13 above, wherein the identifier is a station class mark.

24. The invention as set forth in claim 13 above, wherein the comparing step further comprises comparing secondary patterns characteristic of the radiotelephone to stored identifiers of the secondary patterns to determine whether the radiotelephone is fraudulent, when the comparison of the digital RF signature indicates a close, but not exact, match, wherein the secondary patterns comprise one or more of the following:

a mobile identification number (MIN) transmitted from the radiotelephone,

an electronic serial number (ESN) transmitted from the radiotelephone,

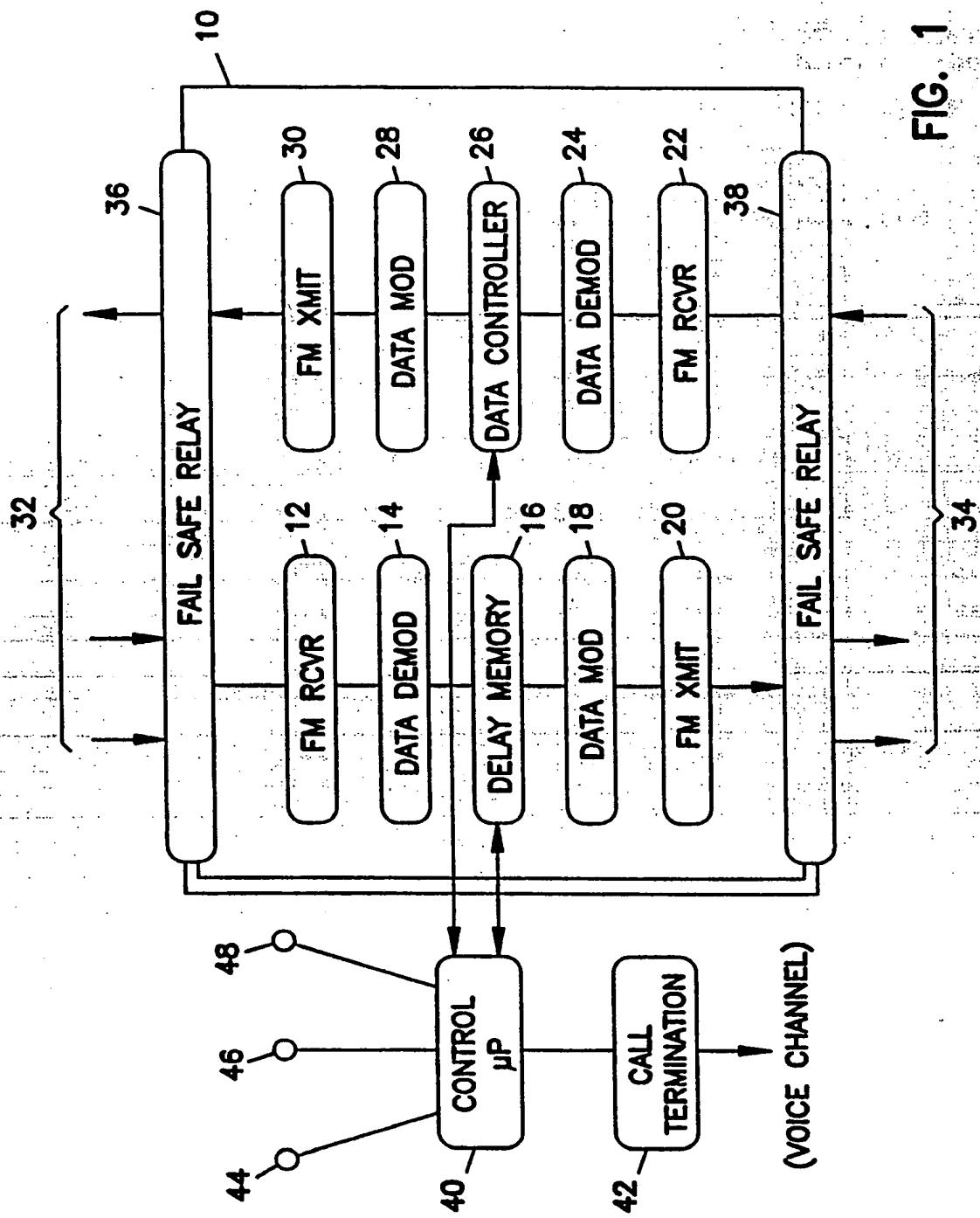
a called number transmitted from the radiotelephone,

a receiving site receiving the call origination request,

a frequency of call origination requests received from the radiotelephone for a specified time period, and

an amount of time the radiotelephone has been in use for a specified time period.

1 / 3



SUBSTITUTE SHEET (RULE 26)

2 / 3

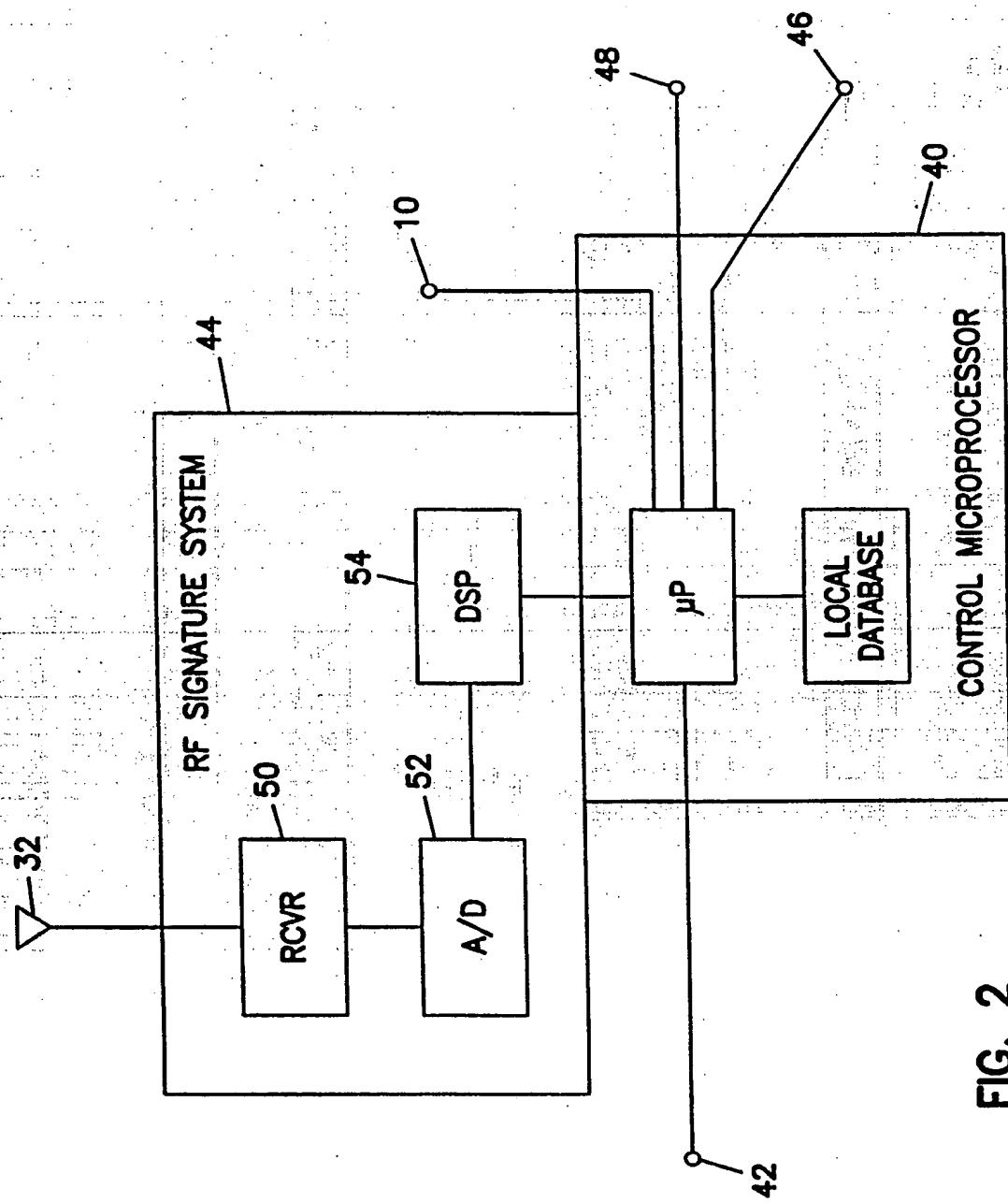


FIG. 2

SUBSTITUTE SHEET (RULE 26)

3 / 3

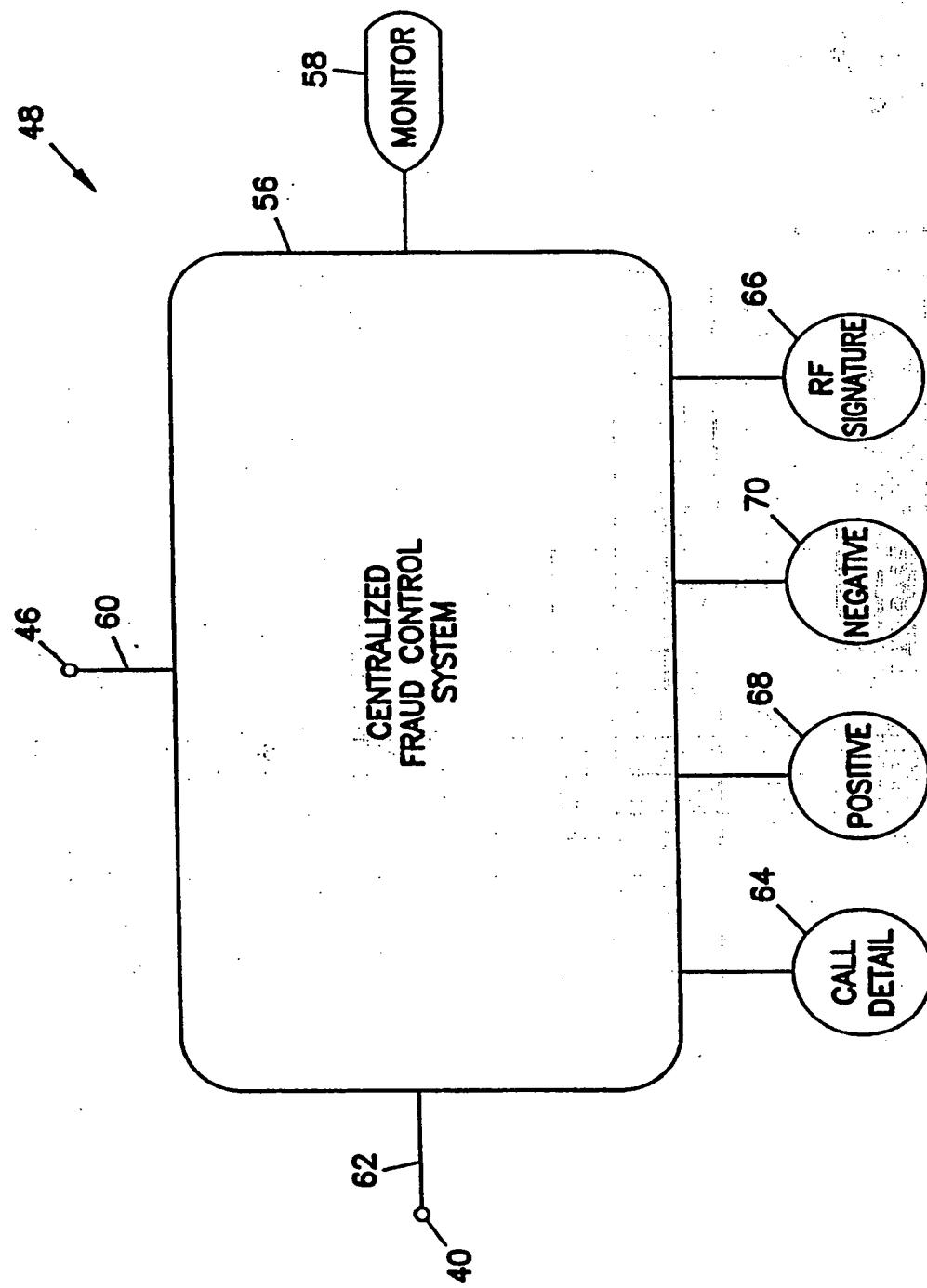


FIG. 3

SUBSTITUTE SHEET (RULE 26)

A. CLASSIFICATION OF SUBJECT MATTER

H 04 Q 7/30

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H 04 Q, H 04 B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	DE, A1, 3 402 467 (SIEMENS) 01 August 1985 (01.08.85), fig. 1,2; page 3, line 13 - page 4, line 4.	1,13
A	EP, A2, 0 163 358 (PHILIPS PATENTVERWALTUNG) 04 December 1985 (04.12.85), abstract.	1,13
A	US, A, 5 005 210 (FERRELL) 02 April 1991 (02.04.91), fig. 1; abstract (cited in the application).	1,13
A	WO, A1, 93/09 640 (ELECTRONIC DATA SYSTEMS)	1,13

 Further documents are listed in the continuation of box C. Patent family members are listed in annex.

Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search

30 June 1994

Date of mailing of the international search report

03.08.94

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentaan 2
NL - 2280 HV Rijswijk
Tel. (+ 31-70) 340-2040, Tx. 31 651 epo nl,
Fax (+ 31-70) 340-3016

Authorized officer

DRÖSCHER e.h.

C(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

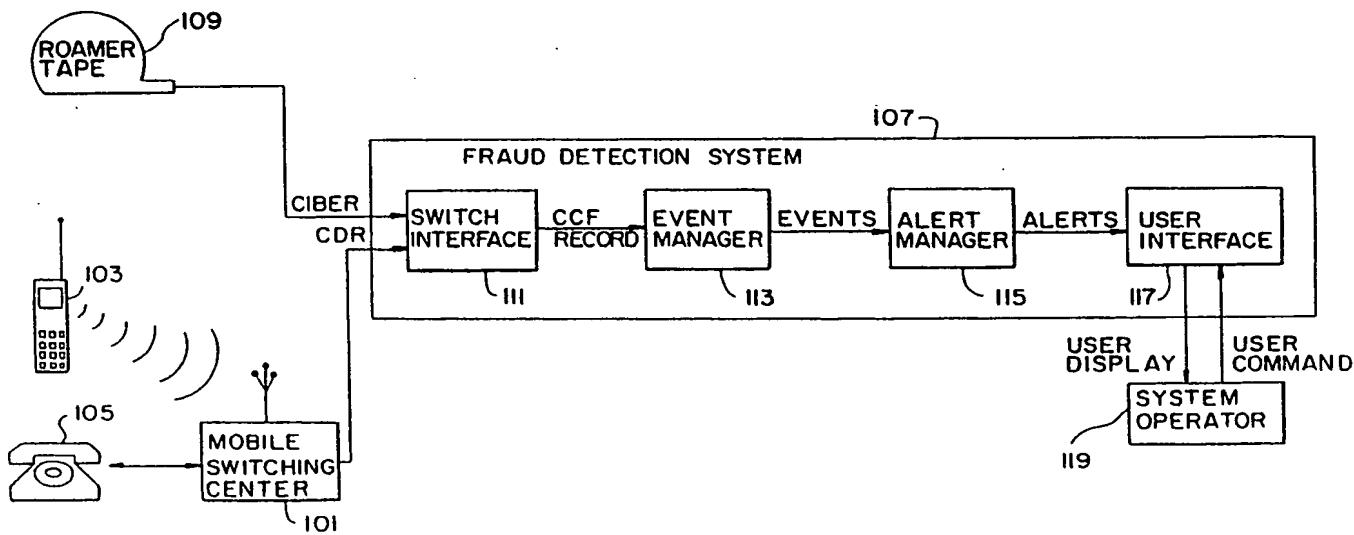
Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	<p>13 May 1993 (13.05.93), fig. 1; abstract. -----</p>	

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 5 :		(11) International Publication Number:	WO 94/11959
H04B 17/00	A1	(43) International Publication Date:	26 May 1994 (26.05.94)

(21) International Application Number:	PCT/US93/10757	(74) Agents:	KULISH, Christopher, J. et al.; Sheridan Ross & McIntosh, 1700 Lincoln Street, 35th Floor, Denver, CO 80203 (US).
(22) International Filing Date:	9 November 1993 (09.11.93)	(81) Designated States:	AT, AU, BB, BG, BR, BY, CA, CH, CZ, DE, DK, ES, FI, GB, HU, JP, KP, KR, KZ, LK, LU, LV, MG, MN, MW, NL, NO, NZ, PL, PT, RO, RU, SD, SE, SK, UA, UZ, VN, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).
(30) Priority data:	975,512 12 November 1992 (12.11.92) US	(73) Applicant:	CORAL SYSTEMS, INC. [US/US]; 1500 Kansas Avenue, Suite 2E, Longmont, CO 80501 (US).
(72) Inventors:	JOHNSON, Eric, A. ; 8015 North 63rd Street, Longmont, CO 80501 (US). LISS, Michael, D. ; 881 Pinegrade Road, Nederland, CO 80466 (US). JENSEN, Flemming, B. ; 9775 Deer Brook Circle, Sandy, UT 84092 (US).	(75) Published	<i>With international search report. Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.</i>

(54) Title: AN APPARATUS AND METHOD FOR DETECTING POTENTIALLY FRAUDULENT TELECOMMUNICATION ACTIVITY



(57) Abstract

An apparatus for detecting potentially fraudulent telecommunication activity, comprising a digital computer (107); interface means (111), operatively connected to the digital computer (107), for receiving a call information record for each call involving a particular subscriber; comparison means, operating within the digital computer (107), for comparing a parameter of the particular subscriber's current usage with a subscriber-specific pattern of the particular subscriber's historical usage; and output means for outputting an indication of a potentially fraudulent call based upon a result of the comparison performed by the comparison means.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	GB	United Kingdom	MR	Mauritania
AU	Australia	GE	Georgia	MW	Malawi
BB	Barbados	GN	Guinea	NE	Niger
BE	Belgium	GR	Greece	NL	Netherlands
BF	Burkina Faso	HU	Hungary	NO	Norway
BG	Bulgaria	IE	Ireland	NZ	New Zealand
BJ	Benin	IT	Italy	PL	Poland
BR	Brazil	JP	Japan	PT	Portugal
BY	Belarus	KE	Kenya	RO	Romania
CA	Canada	KG	Kyrgyzstan	RU	Russian Federation
CF	Central African Republic	KP	Democratic People's Republic of Korea	SD	Sudan
CG	Congo	KR	Republic of Korea	SE	Sweden
CH	Switzerland	KZ	Kazakhstan	SI	Slovenia
CI	Côte d'Ivoire	LI	Liechtenstein	SK	Slovakia
CM	Cameroon	LK	Sri Lanka	SN	Senegal
CN	China	LU	Luxembourg	TD	Chad
CS	Czechoslovakia	LV	Latvia	TG	Togo
CZ	Czech Republic	MC	Monaco	TJ	Tajikistan
DE	Germany	MD	Republic of Moldova	TT	Trinidad and Tobago
DK	Denmark	MG	Madagascar	UA	Ukraine
ES	Spain	ML	Mali	US	United States of America
FI	Finland	MN	Mongolia	UZ	Uzbekistan
FR	France			VN	Viet Nam
GA	Gabon				

AN APPARATUS AND METHOD FOR DETECTING POTENTIALLY FRAUDULENT TELECOMMUNICATION ACTIVITY

Background of the Invention

1. Field of the Invention

5 This invention relates to monitoring telecommunication systems, and more specifically, to an apparatus and method for detecting potentially fraudulent telecommunication system usage. Telecommunication systems include both wireless systems (e.g., cellular telephones, satellite 10 transmission, etc.) and systems utilizing transmission lines (e.g., common telephone systems). Fraudulent telecommunication activity is unauthorized usage for which the telecommunication system owner is not paid for its services.

15 2. Description of the Related Art

Because immediate access to information has become a necessity in virtually all fields of endeavor -- including business, finance and science -- telecommunication systems usage, particularly for wireless telecommunication systems, 20 is increasing at a substantial rate. With the increase in overall usage, however, the incidence of fraudulent usage has experienced a corresponding increase. It is estimated, for example, that fraudulent wireless telecommunication system usage is responsible for losses to the wireless 25 telecommunication industry of \$600 million each year. Clearly, a system for detecting and preventing such fraudulent activity would be highly desirable.

Fraudulent telecommunication activity, which may occur both in wireless and common telephone systems, has

-2-

several different varieties. Among these varieties are cloning fraud, tumbling fraud, tumbling-clone fraud, calling card fraud, and subscriber fraud.

5 Cloning fraud, which occurs in cellular telephone systems, involves the misappropriation of a valid set of subscriber identification numbers (ID), programming the ID into one or more cellular telephones, and then using the "cloned" cellular telephones to place calls which are billed to the subscriber whose ID was misappropriated.

10 Tumbling fraud involves placing cellular telephone calls using a different randomly generated subscriber ID for each telephone call placed. Under certain circumstances no pre-call verification of the ID number is performed before the call is connected. Therefore, a 15 fraudulent user may place calls even without possession of a valid subscriber ID. In this way, for example, 50 fraudulent calls placed by a single fraudulent user will be billed to 50 different subscriber IDs, most of which will be unassigned and unbillable, rather than to a single 20 subscriber as in the case of cloning fraud.

Tumbling-Clone fraud, as the name suggests, is a hybrid of tumbling fraud and cloning fraud which involves placing cellular telephone calls using a plurality of cloned subscriber IDs. For example, a tumbling-clone 25 cellular telephone may have a sequence of 10 different cloned subscriber IDs programmed into it. With each successive call placed by the fraudulent user, the cellular telephone would use the cloned subscriber ID next in

-3-

sequence to initiate the call. In this way, the fraudulent calls would equally be dispersed over 10 different subscriber IDs, consequently making the fraudulent activity more difficult to detect.

5 Calling card fraud involves the misappropriation of a valid calling card number and then using the misappropriated number to place toll calls which are billed to an unsuspecting subscriber.

10 Subscriber fraud, which may occur in either cellular telephone or common telephone systems, involves fraudulent usage by an otherwise legitimate subscriber. Typically, this type of fraud is experienced when a subscriber signs up for telecommunication services, either cellular or calling card, and proceeds to use the telecommunication 15 services with no intent of ever paying for the services provided. A user practicing subscriber fraud would continue to use the services without paying until system access was blocked by the service provider.

20 Although a number of prior fraud detection and prevention systems have been suggested, all have proved inadequate for various reasons. One proposed solution involves setting a predetermined number as a system-wide threshold for the number of cellular calls that may be placed by an individual subscriber in one day; when the 25 predetermined number is exceeded, the method indicates that fraud has occurred. The system-wide threshold method, however, has several drawbacks. For example, this method applies the same threshold to every user. Typically, a

-4-

high-volume subscriber such as a stockbroker may regularly place a large volume of calls each day in the normal course of business, whereas a low-volume subscriber who maintains a cellular telephone primarily for emergency usage may only 5 place a few calls each week. The system-wide threshold method would be inadequate for each of these users, because it would generate a false alert for the high-volume subscriber who happens to legitimately exceed the threshold on a given day, while, incorrectly, no alert would be 10 generated for the fraudulent use of the low-volume subscriber ID, as long as the threshold was not exceeded. Moreover, the system-wide threshold method is easily defeated by a fraudulent user who is aware of the predetermined threshold and takes care to limit the number 15 of fraudulent calls placed to a number less than the threshold.

Another method, referred to as "call numbering," has been proposed to detect fraudulent cellular telephone calls, wherein a predetermined sequence of numbers is 20 assigned to each cellular telephone unit within the network and, with each successive call placed, the next number in sequence is transmitted by the cellular telephone unit to the service provider station and recorded in the order received. When the call records are processed, if any call 25 sequence number occurs more than once, or if the call sequence numbers are out of order, fraud or malfunction is indicated and the cause must be investigated. This method, however, has the disadvantage, *inter alia*, of requiring

-5-

that the cellular telephone unit be modified to include additional equipment to generate and transmit the predetermined sequence of numbers. Consequently, the "call numbering" method is incompatible with the large majority of existing telecommunication equipment that has not been modified.

Moreover, the call numbering method is unreliable. It has been found that the call number sequence may become disordered through normal legitimate use, by events such as 10 early termination of the call or power failure, thereby resulting in false alerts.

Therefore, a system which reliably and accurately indicates the possibility of fraudulent telecommunication activity, but which is flexible enough to permit legitimate 15 use by a wide variety of subscribers, and which is compatible with all types of existing telecommunication equipment is needed.

Summary of the Invention

It is an object of the present invention to provide a 20 method and apparatus for detecting potentially fraudulent telecommunication activity by comparing current usage for a particular subscriber ID or calling card number with the particular subscriber's historical pattern of usage. If current usage for that ID or calling card number indicates 25 a deviation in the historical pattern of usage by the subscriber, a potential fraud is indicated.

-6-

In one embodiment of the invention, the particular subscriber's usage is analyzed to determine parameters such as call duration (the average length in time of a call), call velocity (the number of calls placed within a specified time period), and call thresholds (the highest number of calls placed by the subscriber within a specified time period). One or more of these parameters is then compared to the particular subscriber's historical pattern of usage. If there is abnormal usage relative to the subscriber's historical pattern of usage, a potential fraud is indicated.

In one embodiment a particular subscriber's usage is characterized as a plurality of moving averages, each calculated over a different specified number of days, which are then compared to each other to determine if a significant deviation in usage has occurred. When a significant deviation in usage is detected, a potential fraud is indicated.

In another embodiment, a significant deviation in usage is indicated when both of the following two conditions are satisfied: (1) a moving average calculated over a shorter number of days is greater than a moving average calculated over a longer number of days; and (2) the percentage increase between a moving average calculated on day (t) and the same moving average calculated on the prior day (t-1) exceeds a predetermined amount.

It is a further object of the present invention to provide a method and apparatus for detecting potentially

-7-

fraudulent telecommunication activity by detecting an occurrence of overlapping calls. Overlapping calls are two or more calls which either (1) occur concurrently, or (2) are placed from different geographic regions and occur 5 within a sufficiently short time interval such that it would be improbable that a single subscriber could place the first call and then travel to the location of the second call within the given time interval to place the second call. Because each unique subscriber ID or calling 10 card number may typically only be used by a single subscriber from a single location at one time, fraud is indicated upon occurrence of either or both of these two conditions.

In one embodiment, the fraud detection apparatus looks 15 at each call made by a particular subscriber to determine whether any two calls using the same subscriber ID or calling card number occurred substantially concurrently.

In another embodiment, the fraud detection apparatus adjusts each call for geographic dispersion to determine if 20 two or more calls were placed using the same subscriber ID or calling card number from different geographic locations within a sufficiently short time interval such that travel between the two geographic locations within the given time interval is improbable.

25 It is a further object of the present invention to provide a method and apparatus for detecting potentially fraudulent telecommunication activity by comparing the particular subscriber's present telecommunication usage

-8-

with a predetermined call destination. If the predetermined subscriber-specific condition is satisfied, fraud is indicated.

5 In one embodiment, each number called using a particular subscriber ID or calling card number is compared to a predetermined list of numbers suspected of frequently being called by fraudulent users.

10 In a further embodiment, each country called using a particular subscriber ID or calling card number is compared to a predetermined list of countries suspected of frequently being called by fraudulent users.

15 Several of the above-mentioned objects are achieved by an apparatus comprising a digital computer; interface means for receiving a call information record for each call involving a particular subscriber; comparison means for comparing the particular subscriber's current usage with a subscriber-specific historical pattern of usage; and output means for outputting an alert-state to signal a potentially fraudulent call based upon a result of the comparison 20 performed by the comparison means.

These and other features of the present invention will become evident from the detailed description set forth hereafter with reference to the accompanying drawings.

Brief Description of Drawings

25 A more complete understanding of the invention can be had by referring to the detailed description of the invention and the drawings in which:

-9-

FIG. 1A is a diagram illustrating a typical cellular telecommunications network.

FIG. 1B is a block diagram of a telecommunications fraud detection system according to one embodiment of the 5 present invention.

FIG. 2 is a block diagram showing the components of a Common Call Format (CCF) record according to one embodiment of the present invention.

FIGS. 3A-3L are flowcharts of the Event Manager 10 procedure.

FIGS. 4A-4L are flowcharts of the Alert Manager procedure.

FIGS. 5A-5C are flowcharts of the User Interface procedure.

15 FIG. 6 is a screen display of the Login Window of the User Interface in one embodiment of the present invention.

FIG. 7 is a screen display of the Control Window of the User Interface in one embodiment of the present invention.

20 FIG. 8 is a screen display of the Investigate Subscriber Window of the User Interface in one embodiment of the present invention.

FIG. 9 is a graph showing call velocity fluctuations for a typical cloning fraud user.

25 FIG. 10 is a screen display of the Monitor New SID(s) Window of the User Interface in one embodiment of the present invention.

-10-

FIG. 11 is a screen display of the Monitor Alerts Window of the User Interface in one embodiment of the present invention.

Detailed Description of the Invention

5 A detailed description of an apparatus and method for detecting potentially fraudulent telecommunications activity, is set forth below with reference to the figures.

A diagram illustrating a typical cellular telecommunications network is illustrated in FIG. 1A.

10 Referring to FIG. 1A, each predetermined fixed geographic region is served by a separate Mobile Switching Center (MSC). Additionally, each MSC region may comprise one or more cells, wherein each cell is served by its own base station connected to the MSC for that region. In FIG. 1A,

15 Region I is served by a first MSC 101 while Region II is served by a second MSC 102. Region I comprises four cells each having its own base station 104 connected to the first MSC 101. Region II comprises three cells each having its own base station 106 connected to the second MSC 102.

20 When a subscriber originates a call, the cellular telephone 103 communicates via a base station with the particular MSC serving that geographic region by means of wireless radiofrequency transmission. The subscriber may either remain within the particular cell from which the 25 call was originated or the subscriber may roam across cell and MSC region boundaries. For example, a cellular call may be originated by a subscriber in Cell A and the call

-11-

would be handled initially by the first MSC 101. However, because cellular telephones are mobile, the subscriber could travel from Cell A into Cell B during the course of the call. Upon crossing from Cell A into Cell B, the call 5 would cease being handled by the first MSC 101 and may be picked up mid-call and handled by the second MSC 102.

Multiple MSCs are dispersed throughout the United States, and much of the world, so that a subscriber may call from any geographic region served by a MSC. All of 10 the various MSCs around the world are interconnected by a global telecommunications network, so that telecommunications may occur between two cellular telephones, or between a cellular telephone and a physical line telephone, even if they are in different geographic 15 regions.

The function of a MSC is to receive and route both cellular originated calls and cellular terminated calls. A cellular originated call is one placed by a cellular telephone located within the MSC serving area to either 20 another cellular telephone or a physical line telephone. A cellular terminated call is one received by a cellular telephone located within the MSC serving area, regardless if placed by a cellular or physical line telephone.

Each subscriber's cellular telephone has its own 25 unique ID corresponding to a set of identification numbers. The identification numbers comprise two individual identifiers -- a Mobile Identification Number (MIN), and (2) a Mobile Serial Number (MSN). The MIN is a ten-digit

-12-

number, corresponding to the ten-digit telephone number used in North America, having the format npa-nxx-xxxx, where npa is a three-digit area code, nxx is a three-digit prefix which identifies the serving switch, and xxxx is a four-digit suffix which identifies the individual subscriber or physical line number. The combination of the npa and nxx components form a number which identifies a subscriber's "home" MSC. At the initiation of each call, the cellular telephone transmits to the MSC its unique combination of MIN and MSN. For each call, whether cellular originated or cellular terminated, each MSC handling the call creates a separate Call Detail Record (CDR) which contains several items of information describing the call and the subscriber. For example, the CDR contains the following call information items: MIN, MSN, number called, call duration, call origination date and time, country called, information identifying the MSC, etc. The format of the CDR, however, is not consistent among the several different providers of cellular telephone service. At present, for example, at least five different CDR formats exist.

As mentioned above, each individual subscriber has a single home MSC corresponding to the npa and nxx components of the subscriber's MIN. Unless a cellular subscriber has previously notified the home MSC of his or her whereabouts, the subscriber may only receive a cellular terminated call when that subscriber is within his or her home MSC region.

In most cases, a subscriber may initiate a cellular

-13-

originated call, however, from any MSC region without any special proactive requirements. A subscriber who originates a cellular call from a region other than his or her home MSC region is referred to as a "roamer." Because only the subscriber's home MSC maintains a database of that subscriber's identity and status, a MSC handling a roamer call is unable to verify whether or not the subscriber MIN and MSN received for a call are valid. Accordingly, for each roamer call handled by a MSC, the MSC records CDR information for that call and sends the information to a clearing house. The clearing house collects all CDRs pertaining to a particular MSC, creates a magnetic tape -- a roamer tape -- containing multiple CDRs, and sends the tape to the appropriate home carrier.

FIG. 1B is a block diagram of a telecommunications fraud detection system according to one embodiment of the present invention. Initially, a general description of the fraud detection system 107 is provided as follows.

The fraud detection system 107 of the present invention, comprising the switch interface 111, the event manager 113, the alert manager 115, and the user interface 117, is implemented, in one embodiment, as software running on a digital computer, for example, a Sun Microsystems workstation. The digital computer includes memory means for storing computer programs and data; processing means for running computer programs and manipulating data; and input/output means for communicating with a MSC, a system

-14-

operator, a magnetic tape drive (not shown), or another computer (not shown).

CDR records for both cellular originated and cellular terminated calls fed into a switch interface 111 both from 5 the MSC 101 directly and from a roamer tape 109. After the switch interface 111 translates a CDR record into a format understandable to the fraud detection system 107 -- the CCF format -- a CCF record is passed to the event manager 113. The function of the event manager 113 is to perform a 10 number of checks to compare the present CCF record both with past subscriber-specific usage information and with certain predetermined conditions to determine whether this particular CCF record should trigger the event manager 113 to generate an "event." If an event is generated by the 15 event manager 113 it is logged to a database -- the "events database" -- containing past events specific to each subscriber and passed to the alert manager 115. Depending on the nature and quantity of past events for a particular subscriber, a newly received event may cause the alert 20 manager 115 to generate an "alert" for the particular subscriber ID in question. Each of the alerts generated is stored in a database -- the "alerts database" -- specific to each subscriber. Depending upon a predetermined set of rules, either a single alert or a specific combination of 25 alerts may generate an "alert-state" which is passed to the user interface 117 to signal the system operator 119 that the particular subscriber ID for which the alert-state was generated is suspected of being used fraudulently. Each of

-15-

the alert-states generated is stored in a database -- the "alert-states database" -- specific to each subscriber. The system operator 119 may then investigate a subscriber 5 ID for which an alert-state was generated by looking at subscriber-specific data, a graph of the particular subscriber's call velocity for a given time period, and the history of alerts and events which eventually triggered the alert-state in question. Once the system operator "clears" an alert it will no longer be considered in determining 10 whether an alert-state should be generated for a particular subscriber ID.

Referring to FIG. 1B, a more detailed description of the fraud detection system 107 is provided as follows. A cellular telephone 103 communicates with a MSC 101 to place 15 a call either to a physical line telephone 105 or to another cellular telephone. Additionally, the cellular telephone 103 may receive a call originated by either a physical line telephone 105 or another cellular telephone. The MSC 101 creates a separate CDR record for each call 20 that it handles, whether cellular originated or cellular terminated. Each individual MSC 101 is connected to a fraud detection system 107 which receives CDR records as input from the MSC. The CDR input read directly from the MSC 101 into the fraud detection system 107 corresponds to 25 calls handled by that MSC for its home subscribers. CDR records not involving the MSC's home subscribers are sent to a clearing house to generate roamer tapes to be sent to the appropriate home MSC, as discussed above.

-16-

Alternatively, if the fraud detection system 107 was interconnected to one or more "peer" fraud detection systems, i.e., a separate system serving a different MSC, after the switch interface 111 had converted the CDR 5 records into CCF format, the fraud detection system 107 would send those CCF records corresponding to roamer calls to the appropriate peer fraud detection system corresponding to the respective home MSC of each roamer call.

10 Additionally, the fraud detection system 107 receives input from a roamer tape 109 by means of a magnetic tape reader (not shown) in a format referred to as the CIBER format. The combination of the home MSC 101 input and the roamer tape 109 input represents all of the call activity 15 for a MSC's home subscribers, regardless of the geographic region in which the calls were originated or terminated.

The call information input, whether from the roamer tape 109 or from the home MSC 101, is fed into the switch interface 111 of the fraud detection system 107. The 20 function of the switch interface 111 is to translate the various CIBER and CDR input formats into a consistent format -- the Common Call Format (CCF). The switch interface 111 is capable of accepting CDR input in any of the existing formats, and is easily adaptable to new CDR 25 formats created in the future. Typically, a CCF record contains only a subset of the total information contained in a CDR. This subset of information corresponds to those

-17-

information items used during operation of the fraud detection system 107.

Alternatively, in another embodiment of the present invention, the fraud detection system 107 may receive input from a telecommunications system other than a cellular telephone MSC. For example, the fraud detection system may receive input from a calling card system to detect calling card fraud merely by modifying the switch interface 111 to accept the data format specific to the calling card system used.

FIG. 2 illustrates one embodiment of the present invention wherein the CCF Record 201 comprises sixteen separate fields, numbered 203 through 233. The combination of the npa field 203, the nxx field 205, and the xxxx field 15 207 comprise the subscriber's ten-digit telephone number, or MIN, as discussed above. The switch interface 111 separates the MIN into three components so that each may be separately accessed with ease.

The MSN field 209 holds the subscriber Mobile Serial Number (MSN) which, as discussed above, is transmitted along with the MIN by the cellular telephone 103 to the MSC 20 101 with each cellular originated call.

The call type field 211 holds a value of "0" if this call was cellular originated or a value of "1" if this call 25 was cellular terminated.

The answer status field 213 holds a value of "0" if this call was not answered by the party called or a value of "1" if the call was answered.

-18-

The called number field 215 holds the number dialed by the cellular subscriber for this call.

The country code field 217 holds a number corresponding to a unique code for the particular country 5 called by the cellular subscriber for this call.

The roamer status field 219 holds a "TRUE" state if the subscriber was a "roamer" when the call was originated, that is, the subscriber placed the call through a MSC other than his or her home MSC, or a "FALSE" state if the 10 subscriber placed the call from his or her home MSC.

The sid field 221 holds a switch identifier number identifying the serving MSC that generated the present CDR record for this call. Because a subscriber may move between different MSC regions during the course of a single 15 cellular call, multiple MSCs may handle a single call in successive fashion as the subscriber roams between MSC regions. Accordingly, multiple CDR records may be generated for a single call -- one for each MSC that handled the call. The sid field 221 identifies the MSC 20 that generated this particular CDR, even if it was not the MSC on which the call originated.

The first serving MSC field 223 and the first serving cell field 225 identify the specific MSC and cell, respectively, on which the call originated. As discussed 25 above, both the cell and the MSC which handle a call may change as the subscriber roams across cell and MSC region boundaries. Although each MSC which handles a call will generate a separate CDR having its own switch number in the

-19-

sid field 221, the first serving MSC field 223 and the first serving cell field 225 will remain constant for all CDR records pertaining to a single call.

5 The orig time field 227 and the orig date field 229 hold the time and date, respectively, at which the present call was originated.

The call feature field 231 holds information indicating whether this call utilized a call feature, such as call waiting, call forwarding, or three-way calling.

10 Lastly, the call seconds field 233 holds the duration of the present call in seconds.

Referring again to FIG. 1B, once the switch interface 111 has translated the CDR or CIBER format input into a CCF record, it passes the CCF record to the event manager 113. 15 The event manager 113 procedure is illustrated by a flowchart in FIG. 3A. The function of the event manager is to perform a number of checks to compare the present CCF record both with past subscriber-specific usage information and with certain predetermined conditions to determine 20 whether this particular CCF record should trigger an "event."

Referring to FIG. 3A, the services indicated by steps S303 through S309 are referred to as "call event" checks. In the call event checks the CCF record is compared to a 25 set of predetermined conditions to determine whether or not an event should be generated for this CCF record. Call events are further broken down into the following event types: number events, country events, credit events, and

-20-

overlap events. Additionally, overlap events have two event subtypes: geographic dispersion and simultaneous calls.

The services indicated by steps S311 through S321 are referred to as "pattern event" checks. In the pattern event checks the CCF record is used to update a plurality of previously compiled subscriber-specific usage patterns which define a particular subscriber's typical usage. Each CCF record received by the event manager is used to update and maintain an individual usage pattern for the particular subscriber to which the CCF record pertains. In pattern event checks, the event manager will generate an event when the present CCF record, when used to update the subscriber-specific usage pattern, causes the subscriber's usage pattern to indicate a trend of abnormal usage suggestive of fraudulent telecommunications activity. Pattern events are further broken down into the following event types: average events and threshold events. Additionally, average events have the following four subtypes: velocity, international velocity, duration, and international duration. Threshold events have the following six subtypes: daily velocity, daily international velocity, five-day average velocity, five-day average international velocity, ten-day average velocity, and ten-day average international velocity.

The event manager procedure initiates at step S300 when the event manager 113 receives a CCF record from the switch interface 111. At step S301 the event manager parses the CCF record to place the CCF component fields

into appropriate variables and data structures to be easily accessible by the event manager services. It should be noted that due to delays in creating and forwarding roamer tapes to the appropriate home MSC, a CCF record being processed by the fraud detection system on a particular day may actually correspond to a call placed several days earlier. Therefore, for each of the steps performed by the fraud detection system, as discussed below, the CCF record is analyzed based on the day the call was originated, rather than on the date on which the CCF record is processed by the fraud detection system. For the sake of convenience, the date on which a call originated will be referred to as the "call date," while the date on which the CCF record is processed by the fraud detection system will be referred to as "today." The date on which a call originated is determined by the value held by the orig_date field 229 of the CCF record 201. Additionally, the fraud detection system maintains a database of all CCF records received over the past predetermined number of days so that a delayed CCF record can be analyzed in connection with other calls placed on the same day. This database is referred to as the "calls database."

At step S302 the event manager uses the present CCF record to update the subscriber-specific usage patterns. Specifically, the event manager calculates new five-day and ten-day moving averages for each of the call velocity pattern, the international call velocity pattern, the call duration pattern, and the international call duration

-22-

pattern. A moving average is a technique used in time-series analysis to smooth a series or to determine a trend in a series, calculated by the equation:

5 $m_n = \frac{\sum_{k=n+1-d}^n u_k}{d}$

where m_n is the moving average on day n ; k is an index counter; d is the number of days over which the average is calculated and u_1, u_2, \dots, u_n are a series of values to be averaged. For example, assume a series of values over day 21 to day 25 where $u_{21}=16$, $u_{22}=9$, $u_{23}=12$, $u_{24}=8$, and $u_{25}=15$. To calculate a five-day moving average on the 25th day, m_{25} , n is equal to 25, d is equal to 5, and k takes the successive values 21, 22, 23, 24, and 25.

15 Therefore:

$$m_{25} = \frac{u_{21} + u_{22} + u_{23} + u_{24} + u_{25}}{5}$$
$$= \frac{16 + 9 + 12 + 8 + 15}{5}$$
$$= 12.$$

20 Five and ten-day moving averages are calculated for each of the above-listed four patterns in similar fashion. For example, the five-day moving average call velocity is calculated by summing the number of calls originated within the past five days using a particular subscriber ID and dividing the total by five. Of course, the ten-day averages are calculated by summing over ten days and dividing by ten, rather than five. In order to calculate the ten-day moving average, the fraud detection system

saves CCF records for each particular subscriber for the past eleven days.

Although this embodiment of the present invention characterizes subscriber-specific usage patterns by utilizing two moving averages calculated over five days and ten days, respectively, it should be noted that an alternative embodiment may utilize other types of characterizing schemes, for example a weighted moving average. Additionally, even if moving averages are utilized, a different number of moving averages, for example one, three or more, may be used as deemed effective. Moreover, the moving averages may be calculated over a number of days different than five and ten, as desired.

15 Next, the event manager runs the CCF record through a series of call event checks and pattern event checks, represented by steps S303 through S321. Although one embodiment of the present invention arranges these checks in a specific order as illustrated in FIG. 3A, the checks 20 are substantially order independent and may proceed in any convenient order.

In the embodiment of the present invention depicted in FIG. 3A, the event manager performs the checks in the following order: (1) check suspect termination, (2) check 25 suspect country code, (3) check credit limit, (4) check overlap calls, (5) check call duration pattern, (6) check international call duration pattern, (7) check call thresholds, (8) check international call thresholds, (9)

-24-

check call velocity pattern, and (10) check international call velocity pattern. Each of these checks will be described in further detail below with reference to FIGS. 3B-3L.

5 Referring to FIG. 3B, the Check Suspect Termination service S303 is responsible for determining whether the number called by the cellular subscriber is suspected of being called by other fraudulent cellular telephone users. This service receives the called number field 215 of the 10 CCF Record 201 as an argument.

First, at step S325, the service determines whether the present call was cellular originated by examining the call type field 211 of the CCF Record 201. Because this event check is only relevant for cellular originated calls, 15 if the present call was not cellular originated the service flows to step S337, which marks the completion of the Check Suspect Termination service.

If the present call was cellular originated as determined from the call type field 211, the service, at 20 step S327, tests whether the number called, held in the called number field 215, matches a number on a predetermined list of numbers set by the telecommunication service provider and maintained in a database by the fraud detection system 107. If no number on the list is matched 25 the service flows to step S337 and this check is completed.

If a matching number is found the service, at step S329, tests whether the matched number from the database has been flagged as "suspect." If a specified field in the

-25-

database of numbers is marked "TRUE," then the matched number will be determined to be suspect and the service will flow to step S331. Otherwise, if the specified database field is not marked "TRUE," then the service flows 5 to step S337 and the check is completed.

At step S331, it has been determined that a number called using the particular subscriber ID for this CCF Record is a number suspected of being called by other fraudulent users. Accordingly, the service generates a 10 "suspect termination event" by recording the event type, "number event," along with specific information particular to this call in the events database for this particular subscriber ID.

Next, at step S333, the "event context" data structure 15 is built with information specific to this event. The event context data structure contains information including (1) the event type ("number event"); (2) the event subtype (none for this event type); (3) the subscriber ID number (corresponding to the three MIN fields 203, 205, 207 and 20 the MSN field 209); (4) the call date (from the orig date field 229); and (5) the current alert-state (either normal, yellow, or red depending on the nature and quantity of alerts outstanding for this particular subscriber as determined by the alert manger, discussed below).

25 Next, at step S335, the service sends the event context data structure previously built at step S333 to the alert manager 115 to signal the alert manager that a new

-26-

event has been generated and to provide a reference for locating the newly generated event in the events database.

Lastly, the service flows to step S337, where the suspect termination check is completed and the next check in the event manager procedure is initiated.

Referring to FIG. 3C, the Check Suspect Country Code service S305 is responsible for determining whether the country called by the cellular subscriber, as indicated by the country code, is suspected of being called by other fraudulent cellular telephone users. This service receives the called number field 215 of the CCF Record 201 and its related country code as arguments.

First, at step S339, the service determines whether the present call was cellular originated by examining the call type field 211 of the CCF Record 201. Because this event check is only relevant for cellular originated calls, if the present call was not cellular originated the service flows to step S351, and the Check Suspect Country Code service is completed.

If the present call was cellular originated as determined from the call type field 211, the service, at step S341, tests whether the country code called matches a country code on a predetermined list of numbers set by the telecommunication service provider and maintained in a database by the fraud detection system 107. If no country code on the list is matched the service flows to step S351 and this check is completed.

-27-

If a matching country code is found the service, at step S343, tests whether the matched country code from the database has been flagged as "suspect." If a specified field in the database of country codes is marked "TRUE," 5 then the country code will be determined to be suspect and the service will flow to step S345. Otherwise, if the specified database field is not marked "TRUE," then the service flows to step S351 and the check is completed.

At step S345, it has been determined that a country 10 called using the particular subscriber ID for this CCF Record is a country suspected of being called by other fraudulent users. Accordingly, the service generates a "suspect country code event" by recording the event type, "country event," along with specific information particular 15 to this call in the events database for this particular subscriber ID.

Next, at step S347, the event context data structure is built with information specific to this event, as discussed above. The event context data structure for this 20 service has the event type, "country event," and no event subtype.

Next, at step S349, the service sends the event context data structure previously built at step S347 to the alert manager 115 to signal the alert manager that a new 25 event has been generated and to provide a reference for locating the newly generated event in the events database.

-28-

Lastly, the service flows to step S351, where the suspect country code check is completed and the next check in the event manager procedure is initiated.

Referring to FIG. 3D, the Check Credit Limit service 5 S307 is responsible for determining whether a particular subscriber has exceeded his or her specified usage limit by maintaining a running cumulative total usage duration for each subscriber and comparing the running total to a predetermined value set by the telecommunication service provider. This service receives the call seconds field 10 233 from the CCF Record 201 as an argument.

First, at step S353, the service tests whether this particular subscriber has an entry for the present month in the credit limit database maintained by the fraud detection 15 system. If a credit limit entry is not found an inconsistency in the system has been encountered; an error is logged to an error handling server and the service flows to step S367 which marks the completion of the credit limit check.

20 If a credit limit entry is found for this particular subscriber for the present month, the service flows to step S357 where the running monthly usage total for this particular subscriber is updated by adding the usage for the present call, represented by the value held in the call 25 seconds field 233, to the previous monthly usage total for this particular subscriber.

What is claimed is:

1. An apparatus for detecting potentially fraudulent telecommunication activity, comprising:

a digital computer;

5 interface means, operating within said digital computer, for receiving a call information record for each call involving a particular subscriber;

10 pattern means, operating within said digital computer, for using a plurality of said call information record for said particular subscriber to identify a subscriber-specific pattern of historical call usage and relative to which deviations from said historical call usage can be detected that may be indicative of fraudulent call activity;

15 comparison means, operating within said digital computer, for comparing the particular subscriber's current call usage with information relating to said subscriber-specific pattern of historical call usage to identify potentially fraudulent call activity; and

20 output means, operating within said digital computer, for outputting an indication of a potentially fraudulent call activity based upon a result of the comparison performed by said comparison means.

25 2. A telecommunication fraud detection apparatus according to Claim 1, wherein said information relating to said subscriber-specific pattern of historical call usage includes a subscriber-specific pattern of historical call duration usage and said comparison means compares the

-92-

particular subscriber's current call duration usage with said subscriber-specific pattern of historical call duration usage.

3. A telecommunication fraud detection apparatus
5 according to Claim 1, wherein said information relating to said subscriber-specific pattern of historical call usage includes a subscriber-specific pattern of historical call velocity usage and said comparison means compares the particular subscriber's current call velocity usage with
10 said subscriber-specific pattern of historical call velocity usage.

4. A telecommunication fraud detection apparatus according to Claim 1, wherein said information relating to said subscriber-specific pattern of historical call usage
15 includes subscriber-specific call velocity thresholds and said comparison means compares the particular subscriber's current call velocity usage with said subscriber-specific call velocity thresholds.

5. A telecommunication fraud detection apparatus
20 according to Claim 1, wherein said information relating to said subscriber-specific pattern of historical call usage includes a subscriber-specific daily call velocity threshold and said comparison means compares the particular subscriber's current daily call velocity usage with said
25 subscriber-specific daily call velocity threshold.

6. A telecommunication fraud detection apparatus according to Claim 1, wherein said information relating to said subscriber-specific pattern of historical call usage

-93-

includes a subscriber-specific five-day moving average call velocity threshold and said comparison means compares the particular subscriber's current five day moving average call velocity usage with said subscriber-specific five-day
5 moving average call velocity threshold.

7. A telecommunication fraud detection apparatus according to Claim 1, wherein said information relating to said subscriber-specific pattern of historical call usage includes a subscriber-specific ten-day moving average call
10 velocity threshold and said comparison means compares the particular subscriber's current ten day moving average call usage with said subscriber-specific ten-day moving average call velocity threshold.

8. A telecommunication fraud detection apparatus
15 according to Claim 1, wherein said comparison means compares the particular subscriber's current usage with a combination of at least two of the following of said information relating to said subscriber-specific pattern of historical call usage: a subscriber-specific pattern of historical call duration usage, a subscriber-specific pattern of historical call velocity usage, and a subscriber-specific pattern of historical call velocity usage that includes subscriber-specific call velocity thresholds.

25 9. A telecommunication fraud detection apparatus according to Claim 1, wherein at least one of said current call usage and said information relating to said subscriber-specific pattern of historical call usage

-94-

includes a moving average, and said comparison means performs a comparison using said moving average.

10. A telecommunication fraud detection apparatus according to Claim 1, wherein at least one of said current 5 call usage and said information relating to said subscriber-specific pattern of historical call usage includes a five-day moving average, and said comparison means performs a comparison using said five-day moving average.

10 11. A telecommunication fraud detection apparatus according to Claim 1, wherein at least one of said current call usage and said information relating to said subscriber-specific pattern of historical call usage includes a ten-day moving average, and said comparison 15 means performs a comparison using said ten-day moving average.

12. A telecommunication fraud detection apparatus according to Claim 1, wherein at least one of said current call usage and said information relating to said 20 subscriber-specific pattern of historical call usage includes a plurality of moving averages, and said comparison means performs a comparison using said plurality of moving averages.

13. A telecommunication fraud detection apparatus 25 according to Claim 1, wherein said current call usage includes a five-day moving average and said information relating to said subscriber-specific pattern of historical call usage includes a ten-day moving average, and said

comparison means performs a comparison using said five-day moving average and said ten-day moving average.

14. A telecommunications fraud detection apparatus according to Claim 1, wherein said output means, in 5 response to information provided by said comparison means that identifies potentially fraudulent call activity, decides whether or not to output an indication of a potentially fraudulent call according to a predetermined set of rules.

10 15. A telecommunication fraud detection apparatus according to Claim 1, wherein said pattern means further comprises means for characterizing the particular subscriber's current call usage as a first moving average and said subscriber-specific pattern of historical call 15 usage as a second moving average, each calculated over a different specified number of days, wherein said comparison means compares the first moving average to said second moving average to determine if a meaningful increase in usage has occurred.

20 16. A telecommunication fraud detection apparatus according to Claim 15, wherein said said second moving average is calculated over a greater number of days than said first moving average, and

25 wherein said output means outputs an indication of potentially fraudulent call activity, when each of the following two conditions are satisfied: (1) the first moving average is greater than the second moving average; and (2) a percentage increase between the first moving

-96-

average calculated on day (t) and the first moving average calculated on day (t-1) exceeds a predetermined amount.

17. A telecommunication fraud detection apparatus according to Claim 1, wherein said comparison means 5 comprises means for generating an event E, wherein E is a velocity event, a duration event, a velocity threshold event.

18. A telecommunication fraud detection apparatus according to Claim 1, wherein said comparison means 10 comprises means for generating an alert A, wherein A is a doubling velocity alert indicating that the velocity of calls by said particular subscriber has doubled over a predetermined period, a 3-in-5 velocity alert indicating that three velocity-type events have occurred within a five 15 day period that are associated with said particular subscriber, a doubling duration alert indicating that the duration of calls by said particular subscriber has doubled over a predetermined period, a 3-in-5 duration alert indicating that three duration-type events have occurred 20 within a five day period that are associated with said particular subscriber, a daily velocity threshold alert, a 5-day average velocity threshold alert, a 10-day average velocity threshold alert.

-97-

19. An apparatus for detecting potentially fraudulent telecommunication activity, comprising:

a digital computer;

5 interface means, operating within said digital computer, for receiving a call information record for each call involving a particular subscriber;

10 analysis means, operating within said digital computer, for analyzing the particular subscriber's call usage, based upon one or more of said call information record, to identify potentially fraudulent call activity, said analysis means generating or processing information in the course of identifying potentially fraudulent call activity; and

15 output means, operating within said digital computer, for outputting an indication of said potentially fraudulent call activity based upon a result of the analysis performed by said analysis means, and for displaying at least some of said information generated during the analysis that identified said potentially fraudulent call activity so an 20 assessment of said potentially fraudulent call activity can be made.

20. A telecommunication fraud detection apparatus according to Claim 19, wherein said information displayed by said output means includes an event E, wherein E is a 25 velocity event, a duration event, a velocity threshold event, a suspect number event, a suspect country event, a credit event, or an overlap calls event.

-98-

21. A telecommunication fraud detection apparatus according to Claim 19, wherein said information displayed by said output means includes an alert A, wherein A is a doubling velocity alert indicating that the velocity of 5 calls by said particular subscriber has doubled over a predetermined period, a 3-in-5 velocity alert indicating that three velocity events that are associated with said particular subscriber have occurred within a five day period, a doubling duration alert indicating that the 10 duration of calls by a subscriber has doubled over a predetermined period, a 3-in-5 duration alert indicating that three duration-type events that are associated with said particular subscriber have occurred within a five day period, a daily velocity threshold alert, a 5-day average 15 velocity threshold alert, a 10-day average velocity threshold alert, a suspect number alert, a suspect country alert, a credit alert, or an overlap calls alert.

22. A telecommunication fraud detection apparatus according to Claim 19, wherein said information displayed 20 by said output means includes the particular subscriber's status data.

23. A telecommunication fraud detection apparatus according to Claim 19, wherein said information displayed by said output means includes a graph of the subscriber- 25 specific pattern of usage.

-99-

24. A telecommunication fraud detection apparatus according to Claim 19, wherein said information displayed by said output means includes a graph of the particular subscriber's call velocity.

-100-

25. An apparatus for detecting potentially fraudulent telecommunication activity, comprising:

a digital computer;

5 interface means, operating within said digital computer, for receiving a call information record for each call involving a particular subscriber, said call information record derived from a telecommunication switching center that establishes connections between telecommunication devices;

10 comparison means, operating within said digital computer, for comparing the call destination identified in said call information record involving the particular subscriber with a predetermined call destination to identify potentially fraudulent call activity; and

15 output means, operating within said digital computer, for outputting an indication of said potentially fraudulent call activity based upon a result of the comparison performed by said comparison means.

26. A telecommunication fraud detection apparatus according to Claim 25, wherein the predetermined call destination comprises a suspect termination number.

27. A telecommunication fraud detection apparatus according to Claim 25, wherein the predetermined call destination comprises a suspect country code.

-101-

28. An apparatus for detecting potentially fraudulent telecommunication activity, comprising:

a digital computer;

5 interface means, operating within said digital computer, for receiving a call information record for each of at least two calls associated with a particular subscriber and derived from a switching center that establishes calls between telecommunication devices;

10 detection means, operating within said digital computer, for detecting an occurrence of overlapped calls using said call information record for each of said at least two calls, said detection of overlapped calls indicating that calls associated with said particular subscriber were placed in an improbable time sequence that 15 is indicative of potentially fraudulent call activity; and

output means, operating within said digital computer, for outputting an indication of overlapped calls based upon a result of the analysis performed by said analysis means.

29. A telecommunication fraud detection apparatus 20 according to Claim 28, wherein said detection means detects an occurrence of overlapped calls that are substantially simultaneous calls.

30. A telecommunication fraud detection apparatus according to Claim 28, wherein said detection means detects 25 an occurrence of overlapped calls after consideration of geographic dispersion related information derived from said call information record for each of said at least two calls.

-102-

31. A telecommunication fraud detection apparatus according to Claim 28, wherein said detection means further comprises adjusting means for adjusting information derived from at least one of said call information record to 5 account for geographic dispersion between locations of said at least two calls.

32. A telecommunication fraud detection apparatus according to Claim 28, wherein said detection means comprises adjusting means for adjusting information derived 10 from at least one of said call information record to account for geographic dispersion using an airline formula that provides an estimate of the distance between the locations at which said at least two calls are initiated.

-103-

33. An apparatus for detecting potentially fraudulent telecommunication activity, comprising:

a digital computer;

5 interface means, operating within said digital computer, for receiving a call information record for each call involving a particular subscriber;

10 parameter identifying means, operating within said digital computer, for identifying a parameter of the particular subscriber's current call usage based on information extracted from one or more call information 15 records provided by said interface means;

pattern identifying means, operating within said digital computer, for identifying a subscriber-specific pattern of historical call usage based on information extracted from a plurality of said call information 15 records;

20 analysis means, operating within said digital computer, for analyzing the particular subscriber's current call usage to identify potentially fraudulent call activity, said analyzing means generating data in the course of identifying potentially fraudulent activity and using one or more of the following: information relating to the subscriber-specific pattern of historical call usage identified by said pattern identifying means, a value of a 25 call destination parameter identified in a call information record by said parameter identifying means, or values of a call location parameter identified by said parameter identifying means; and

-104-

output means, operating within said digital computer,
for outputting an indication of a potentially fraudulent
call activity based upon a result of the analysis performed
by said analysis means, and for displaying at least a
5 portion of said data generated in the course of the
analysis that identified said potentially fraudulent
activity so an assessment thereof can be made.

-105-

34. A method for detecting potentially fraudulent telecommunication activity, comprising the steps of:

receiving a call information record for each call involving a particular subscriber;

5 identifying a parameter of the particular subscriber's current usage by extracting information from one or more call information records;

developing and maintaining a subscriber-specific historical call usage pattern by cumulatively processing 10 information extracted from a plurality of call information records;

comparing the particular subscriber's current usage to the subscriber-specific historical call pattern to determine a deviation amount therebetween; and

15 outputting an indication of a potentially fraudulent call when the deviation amount exceeds a predetermined limit.

35. A telecommunication fraud detection apparatus according to Claim 1, wherein said current call usage 20 includes a first average of call usage, said information relating to said subscriber-specific pattern of historical call usage includes a second average of call usage, and said comparison means compares said first average of call usage to said second average of call usage.

25 36. A telecommunication fraud detection apparatus according to Claim 1, wherein said current call usage includes a first average of call usage over a first period of time, said information relating to said subscriber-

-106-

specific pattern of historical call usage includes a second average of call usage over a second period of time that is different than said first predetermined period of time, and said comparison means compares said first average of call 5 usage to said second average of call usage.

37. A telecommunication fraud detection apparatus according to Claim 1, wherein said current call usage includes a first average of call usage over a first period of time extending from a first starting point in time, said 10 information relating to said subscriber-specific pattern of historical call usage includes a second average of call usage, said comparison means compares said first average of call usage to said second average of call usage to determine if said first average of call usage exceeds said 15 second average of call usage and, if so, whether said first average exceeds a third average over a second period of time extending from a second starting point in time by a predetermined amount, wherein said first and second periods of time are substantially equal, but said first starting 20 point in time is different than said second starting point in time.

38. A telecommunication fraud detection apparatus according to Claim 1, wherein said information relating to said subscriber-specific pattern of historical call usage 25 includes information relating to a high of call usage, and said comparison means compares the particular subscriber's current call usage to said information relating to a high of call usage.

-107-

39. A telecommunication fraud detection apparatus according to Claim 1, wherein said information relating to said subscriber-specific pattern of historical call usage includes a threshold, said current call usage includes an 5 average call usage over a period of time, and said comparison means compares said average call usage to said threshold.

40. A telecommunication fraud detection apparatus according to Claim 1, wherein said information relating to 10 said subscriber-specific pattern of historical call usage includes information relating to a high of call usage, said current call usage includes an average call usage over a period of time, and said comparison means compares said average call usage to said information relating to a high 15 of call usage.

41. A telecommunication fraud detection apparatus according to Claim 19 wherein said information displayed by said output means includes a plurality of graphs, each graph relating to the particular subscriber's call velocity 20 over a particular period of time.

42. A telecommunication fraud detection apparatus according to Claim 19 wherein information displayed by said output means includes information relating to a group of subscribers within a defined geographical region that 25 includes said particular subscriber.

-108-

43. An apparatus for detecting potentially fraudulent telecommunication activity, comprising:

a digital computer;

5 interface means, operating within said digital computer, for receiving a call information record for each call involving a particular subscriber, said call information record derived from a switching center that establishes connections between telecommunication devices;

10 analysis mean, operating within said digital computer, for receiving said call information record from said interface means and using said call information record in analyzing the particular subscriber's call usage to identify potentially fraudulent call activity; and

15 output means, operating within said digital computer, for outputting an indication of said potentially fraudulent call activity.

44. An apparatus, as claimed in Claim 43, wherein:

20 said analysis means includes pattern means for using a plurality of said call information record for said particular subscriber to develop information relating to a subscriber-specific pattern of historical call usage, and means for comparing current call usage of the particular subscriber to said information relating to said subscriber-specific pattern of historical call usage.

25 45. A telecommunication fraud detection apparatus according to Claim 44, wherein said current call usage includes a first average of call usage, said information relating to said subscriber-specific pattern of historical

call usage includes a second average of call usage, and said comparison means compares said first average of call usage to said second average of call usage.

46. A telecommunication fraud detection apparatus
5 according to Claim 44, wherein said current call usage
includes a first average of call usage over a first period
of time, said information relating to a subscriber-specific
pattern of historical call usage includes a second average
of call usage over a second period of time that is
10 different than said first predetermined period of time, and
said comparison means compares said first average of call
usage to said second average of call usage.

47. A telecommunication fraud detection apparatus
according to Claim 44, wherein said current call usage
15 includes a first average of call usage over a first period
of time that extends from a first starting point, said
information relating to said subscriber-specific pattern of
historical call usage includes a second average of call
usage, and said comparison means compares said first
20 average of call usage to said second average of call usage
to determine if said first average of call usage exceeds
said second average of call usage and, if so, whether said
first average exceeds a third average of call usage that
extends over a second period of time extending from a
25 second starting point by a predetermined amount, wherein
said first and second periods of time are substantially
equal, but said first starting point in time is different
from said second starting point in time.

-110-

48. A telecommunication fraud detection apparatus according to Claim 44, wherein said information relating to said subscriber-specific pattern of historical call usage includes information relating to a high of call usage, and
5 said comparison means compares the particular subscriber's current call usage to said information relating to a high of call usage.

49. A telecommunication fraud detection apparatus according to Claim 44, wherein said information relating to
10 said subscriber-specific pattern of historical call usage includes a threshold, said current call usage includes an average call usage over a period of time, and said comparison means compares said average call usage to said threshold.

15 50. A telecommunication fraud detection apparatus according to Claim 44, wherein said information relating to said subscriber-specific pattern of historical call usage includes information relating to a high of call usage, the current call usage includes an average call usage over a
20 period of time, and said comparison means compares said average call usage to said information relating to a high of call usage.

51. An apparatus, as claimed in Claim 43, wherein:
said analysis means includes means for determining if
25 two or more calls are one of the following: substantially simultaneously overlapped and overlapped after taking into account geographic dispersion.

-111-

52. An apparatus, as claimed in Claim 43, wherein:
said analysis means includes means for comparing call
destination information from said call information record
to a predetermined call destination information.

5 53. An apparatus, as claimed in Claim 43, wherein:
said analysis means includes means for determining if
the particular subscriber has exceeded a credit limit for
said particular subscriber.

FIG. 1A
REGION I
REGION II

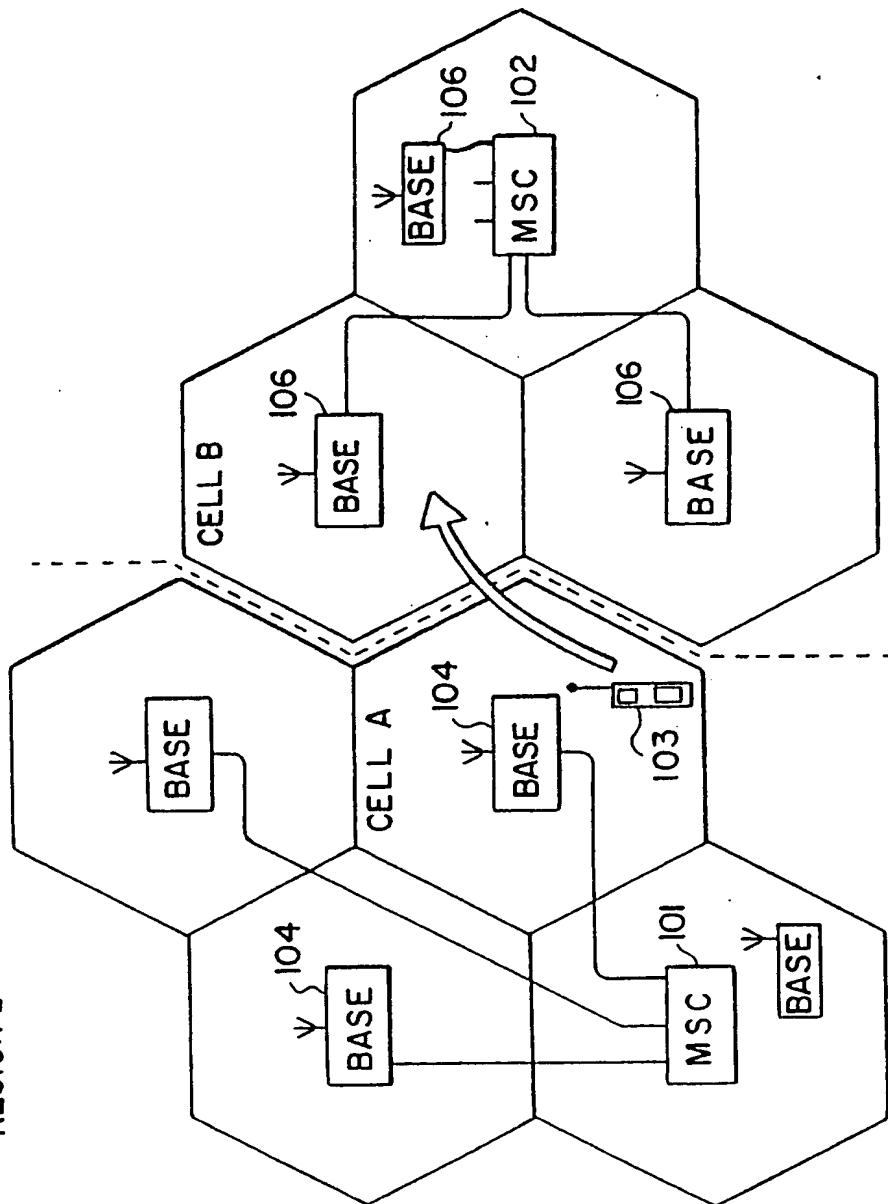


FIG. 1B

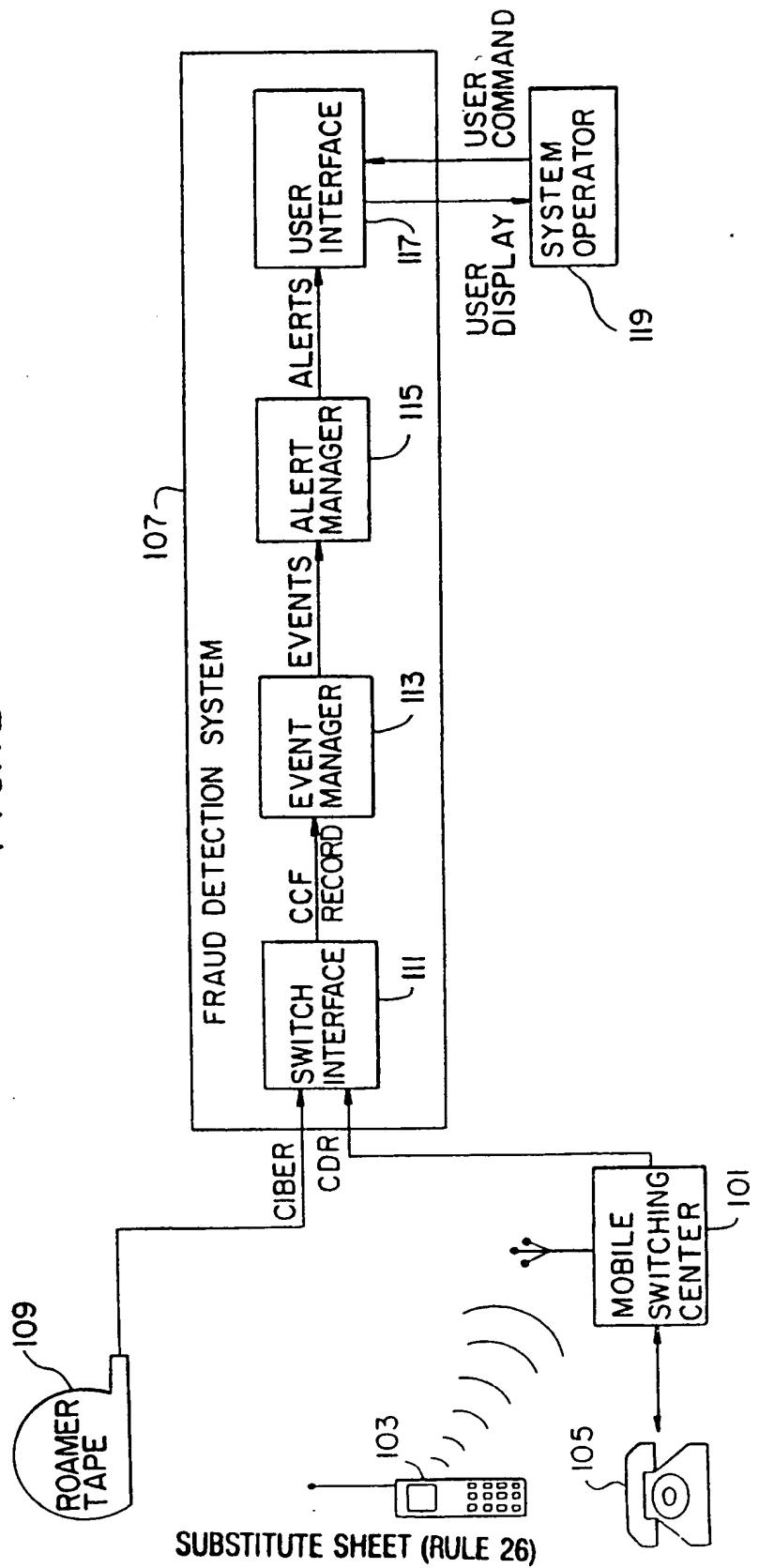


FIG. 2

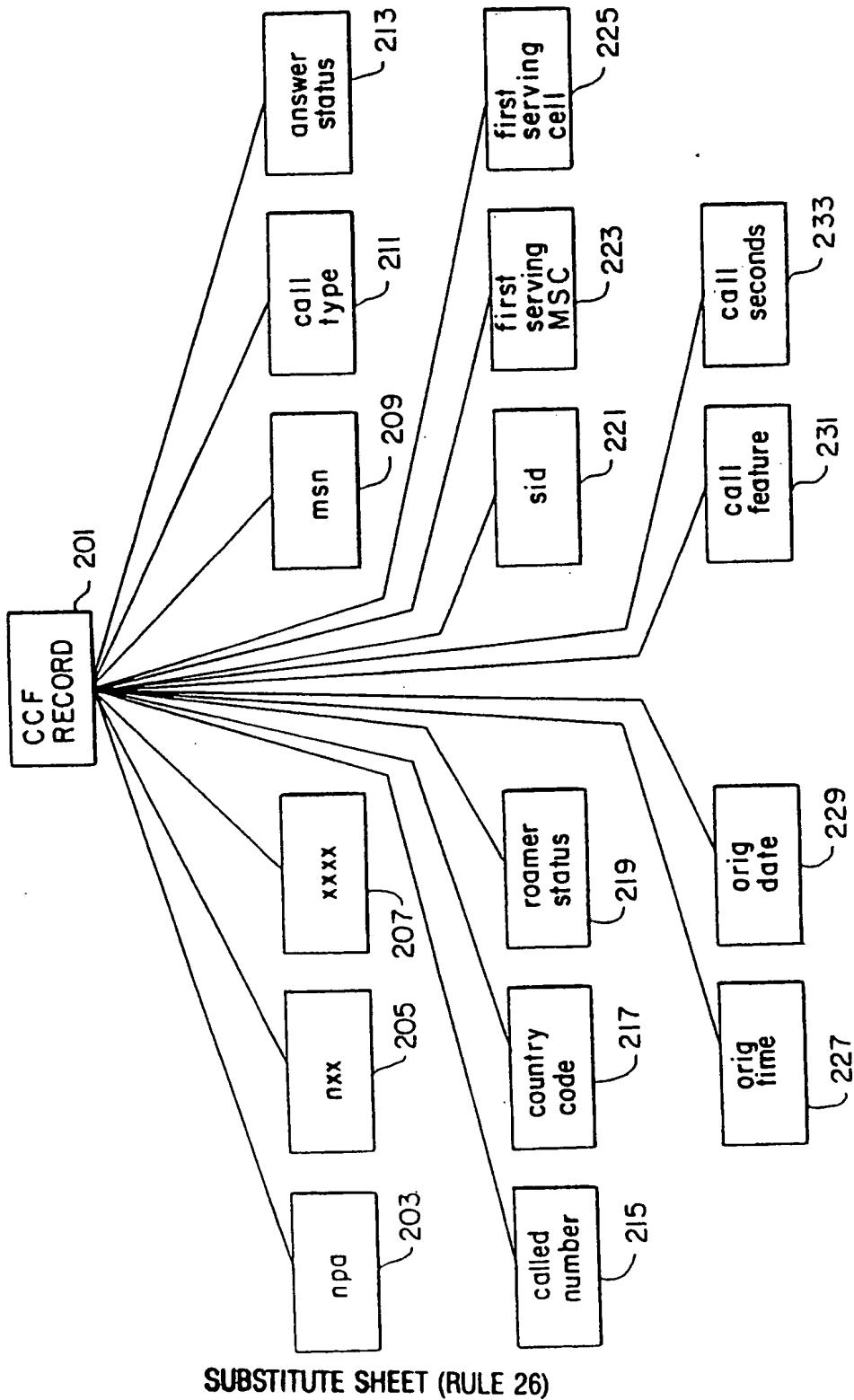
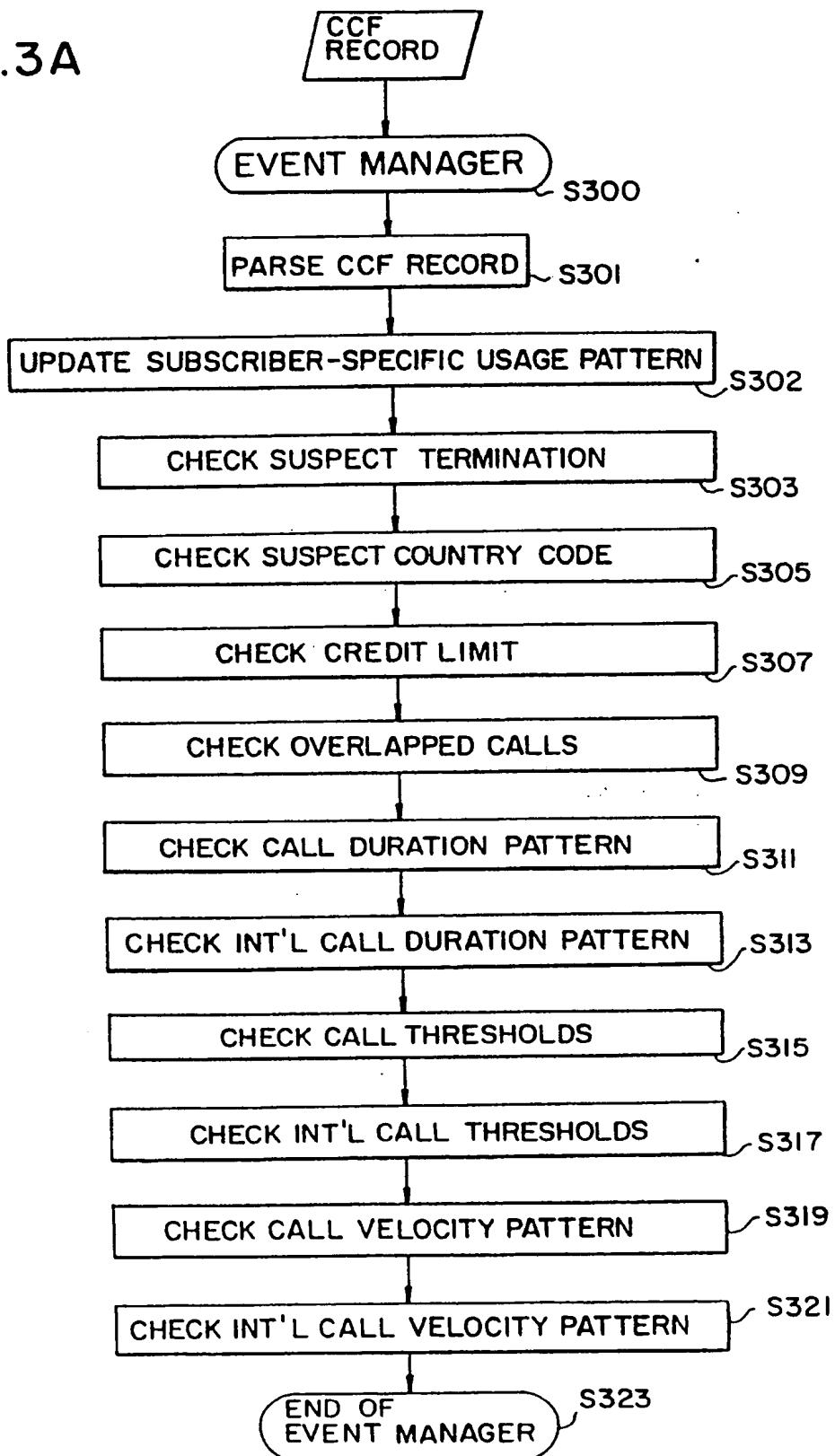


FIG.3A



SUBSTITUTE SHEET (RULE 26)

THIS PAGE BLANK (USPTO)